

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-005526

(43)Date of publication of application : 08.01.2004

(51)Int.Cl. G06F 12/14
G06F 13/00
G06F 17/60
H04L 9/08

(21)Application number : 2003-092488

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 28.03.2003

(72)Inventor : AZUMA AKIO
TOKUDA KATSUMI
OMORI MOTOJI
INOUE MITSUHIRO

(30)Priority

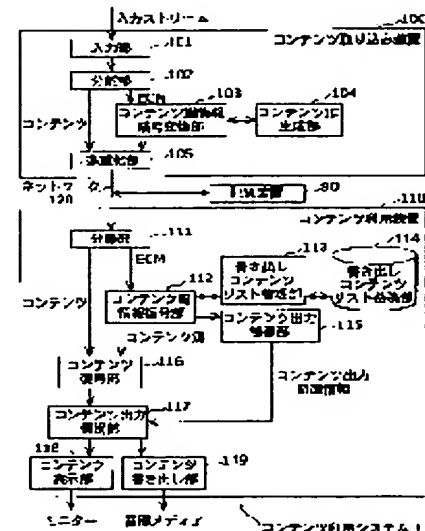
Priority number : 2002103674 Priority date : 05.04.2002 Priority country : JP

(54) CONTENT USING SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a content using system for satisfying mutually opposed requests such as a user request and the protection of a copyright in a well-balanced state on contents bound to a network.

SOLUTION: A content taking-in device 100 has a content ID forming part 104 for forming content ID and a content key information code converting part 103 for converting content key information into a code by a network key. A content using device 110 has a content key information decoding part 112 for decoding the content key information by the network key, a writing-out content list accumulating part 114 for accumulating a list (MCL) for recording the writing-out content ID on an accumulating medium and a writing-out content list control part 113 for determining the possibility of writing-out of the contents on the basis of the MCL.



LEGAL STATUS

[Date of request for examination] 03.02.2006

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

THIS PAGE BLANK (USPTO)

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-5526

(P2004-5526A)

(43) 公開日 平成16年1月8日(2004.1.8)

(51) Int. Cl.⁷

G06F 12/14
G06F 13/00
G06F 17/80
H04L 9/08

F I

G06F 12/14 320E
G06F 12/14 320F
G06F 13/00 540A
G06F 17/60 142
H04L 9/00 601A

テーマコード(参考)

5B017
5J104

審査請求 未請求 請求項の数 35 O L (全 51 頁) 最終頁に続く

(21) 出願番号 特願2003-92488 (P2003-92488)
(22) 出願日 平成15年3月28日(2003.3.28)
(31) 優先権主張番号 特願2002-103674 (P2002-103674)
(32) 優先日 平成14年4月5日(2002.4.5)
(33) 優先権主張国 日本国(JP)

(71) 出願人 000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(74) 代理人 100109210
弁理士 新居 広守
(72) 発明者 東 吾紀男
大阪府門真市大字門真1006番地 松下
電器産業株式会社内
(72) 発明者 徳田 克己
大阪府門真市大字門真1006番地 松下
電器産業株式会社内
(72) 発明者 大森 基司
大阪府門真市大字門真1006番地 松下
電器産業株式会社内

最終頁に続く

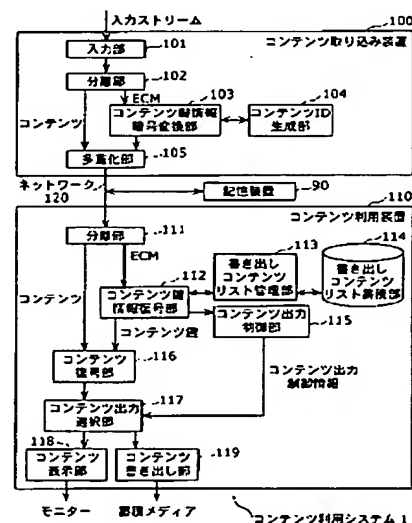
(54) 【発明の名称】 コンテンツ利用システム

(57) 【要約】

【課題】 ネットワークにバインドされたコンテンツについて、ユーザ要求と著作権保護という相対立する要求をバランス良く解決するコンテンツ利用システムを提供する。

【解決手段】 コンテンツ取り込み装置100は、コンテンツIDを生成するコンテンツID生成部104と、ネットワーク鍵でコンテンツ鍵情報を暗号変換するコンテンツ鍵情報暗号変換部103とを備え、コンテンツ利用装置110は、コンテンツ鍵情報をネットワーク鍵で復号するコンテンツ鍵情報復号部112と、蓄積メディアに書き出したコンテンツのIDを記したリスト(MCL)を蓄積する書き出しコンテンツリスト蓄積部114と、MCLに基づきコンテンツの書き出し可否判定を行う書き出しコンテンツリスト管理部113とを備える。

【選択図】 図3



【特許請求の範囲】

【請求項 1】

複数の装置が接続されたネットワークにおいてコンテンツを利用するコンテンツ利用システムであって、

前記複数の装置のうち少なくとも1つの装置に備えられ、コンテンツをネットワーク上の装置のみが利用可能な状態にすることによってコンテンツをネットワークにバインドするバインド手段と、

前記複数の装置のうち少なくとも1つの装置に備えられ、前記バインド手段によってバインドされたコンテンツに対応させてコンテンツIDを発行するID発行手段と、

前記複数の装置のうち少なくとも1つの装置に備えられ、前記バインド手段によってバインドされたコンテンツについて、バインドされた状態を解除するバインド解除手段と、

前記複数の装置のうち少なくとも1つの装置に備えられ、前記バインド解除手段によってバインドを解除されたコンテンツを蓄積メディアに書き出す書き出し手段と、

前記複数の装置のうち少なくとも1つの装置に備えられ、書き出し手段により書き出されたコンテンツのコンテンツIDを示すテーブルを記憶するテーブル手段と、

前記複数の装置のうち少なくとも1つの装置に備えられ、書き出し手段が書き出そうとするコンテンツのコンテンツIDを取得して、前記テーブルの内容に基づいて書き出し手段による当該コンテンツの書き出しを抑制する抑制手段と

を備えることを特徴とするコンテンツ利用システム。

【請求項 2】

前記抑制手段は、書き出し手段が書き出そうとするコンテンツのコンテンツIDを取得し、前記テーブルに当該コンテンツIDが既に記録されていないければ、前記書き出し手段に対して当該コンテンツの書き出しを抑制しないで前記テーブルに取得したコンテンツIDを追加し、前記テーブルに当該コンテンツIDが既に存在していれば、前記書き出し手段に対して当該コンテンツの書き出しを抑制する

ことを特徴とする請求項1記載のコンテンツ利用システム。

【請求項 3】

前記抑制手段は、書き出し手段が書き出そうとするコンテンツのコンテンツIDを取得して、前記テーブルに当該コンテンツIDが存在していなければ、当該コンテンツID及び、書き出し手段による書き出し回数を1として追加し、前記テーブルに当該コンテンツIDが存在し、かつ書き出し回数が予め定められた最大回数に達していれば、書き出し手段による書き出しを抑制することを特徴とする請求項1記載のコンテンツ利用システム。

【請求項 4】

前記バインド手段は、前記複数の装置に共有されているネットワーク鍵を用いて、コンテンツの復号するためのコンテンツ鍵を暗号化することによって、コンテンツをネットワークにバインドする

ことを特徴とする請求項3記載のコンテンツ利用システム。

【請求項 5】

前記複数の装置は、1つのコンテンツ取り込み装置と、少なくとも1つのコンテンツ利用装置とを含み、

前記コンテンツ取り込み装置は前記バインド手段と前記ID発行手段とを備え、

前記各コンテンツ利用装置は前記テーブル手段と前記バインド解除手段と前記書き出し手段と抑制手段とを備える

ことを特徴とする請求項4記載のコンテンツ利用システム。

【請求項 6】

前記コンテンツ利用装置は、さらに、

書き込み手段により書き込みを行った際に少なくとも当該コンテンツIDを他のコンテンツ利用装置に通知する通知手段と、

他のコンテンツ利用装置から通知を受けたときに前記テーブル手段に記憶されたテーブルを更新する更新手段と

を備えることを特徴とする請求項5記載のコンテンツ利用システム。

【請求項7】

前記コンテンツ利用システムは、1つのコンテンツ取り込み装置と、少なくとも1つのコンテンツ利用装置とを含み、

前記コンテンツ取り込み装置は、前記バインド手段と、前記ID発行手段と、前記テーブル手段と、前記抑制手段とを備え、

前記各コンテンツ利用装置は、前記バインド解除手段と前記書き出し手段とを備えることを特徴とする請求項4記載のコンテンツ利用システム。

【請求項8】

前記コンテンツ利用システムは、1つのコンテンツ取り込み装置と、少なくとも1つのコンテンツ利用装置とを含み、

前記コンテンツ取り込み装置は、前記バインド手段と、前記ID発行手段と、前記テーブル手段とを備え、

前記各コンテンツ利用装置は、前記バインド解除手段と、前記書き出し手段と、前記抑制手段とを備える

ことを特徴とする請求項4記載のコンテンツ利用システム。

【請求項9】

前記各コンテンツ利用装置は、さらに

前記コンテンツ取り込み装置のテーブル手段に記憶された前記テーブルの内容を取得することによって、前記テーブルの写しを記憶する第2テーブル手段とを備え、

前記抑制手段は、前記テーブルの写しに基づいて抑制する

ことを特徴とする請求項8記載のコンテンツ利用システム。

【請求項10】

前記コンテンツID発行手段は、(a)～(e)の何れかである

(a)カウンタを用いて前記コンテンツIDを生成して発行する、(b)単調増加、または、単調減少する前記コンテンツIDを生成して発行する、(c)ユニークな値を生成する乱数を用いて前記コンテンツIDを生成して発行する、(d)当該コンテンツと共に配信されるデータに基づいてコンテンツIDを生成して発行する、(e)当該コンテンツと共に配信されるデータからコンテンツIDを取得して発行する

ことを特徴とする請求項4に記載のコンテンツ利用システム。

【請求項11】

前記コンテンツID発行手段は、さらに、

前記コンテンツ取り込み装置を識別するためのIDを関連づけて前記コンテンツID生成する

ことを特徴とする請求項4項に記載のコンテンツ利用システム。

【請求項12】

前記コンテンツID発行手段は、

前記コンテンツIDを、放送番組に対応するコンテンツ毎に生成する

ことを特徴とする請求項4に記載のコンテンツ利用システム。

【請求項13】

前記テーブルは、コンテンツID毎にコンテンツの書き出し先を示す情報を含み、

前記抑制手段は、前記情報が示す書き出し先と、書き出し手段が書き出そうとする書き出し先とが異なる場合は、書き出しを抑制する

ことを特徴とする請求項4記載のコンテンツ利用システム。

【請求項14】

前記テーブルは、コンテンツID毎にコンテンツの書き出し形態を示す情報を含み、

前記抑制手段は、前記情報が示す書き出し形態と、書き出し手段が書き出そうとする書き出し形態とが異なる場合は、書き出しを抑制する

ことを特徴とする請求項4記載のコンテンツ利用システム。

【請求項15】

10

20

30

40

50

前記テーブルは、コンテンツの単位時間あたりの書き出し可能回数の情報を含み、
前記抑制手段は、書き出し手段による単位時間あたりコンテンツ書き出し回数が、単位時間あたりの書き出し可能回数を超えている場合は、書き出しを抑制することを特徴とする請求項4記載のコンテンツ利用システム。

【請求項16】

前記テーブルは、コンテンツの書き出し完了から、次にコンテンツを書き出し開始可能となる迄の時間間隔の情報を含み、
前記抑制手段は、書き出し手段によるコンテンツ書き出しの時間間隔が、前記時間間隔より短い場合は、書き出しを抑制することを特徴とする請求項4記載のコンテンツ利用システム。

【請求項17】

前記テーブルのハッシュ値を、前記テーブル手段でセキュアに管理することを特徴とする請求項4記載のコンテンツ利用システム。

【請求項18】

前記テーブル手段は、前記テーブルに記録されたコンテンツIDを削除するためのしきい値を記憶し、前記テーブルに記録されたコンテンツIDの数が前記しきい値に達したとき、前記テーブルから少なくとも1つのコンテンツIDを削除することを特徴とする請求項4記載のコンテンツ利用システム。

【請求項19】

前記テーブルは、さらに、コンテンツIDを登録した日時を示す日時情報を記録し、
前記テーブル手段は、前記テーブルに記録されたコンテンツIDの数が前記しきい値に達したとき、前記日時情報に基づいて削除すべきコンテンツIDを決定することを特徴とする請求項18に記載のコンテンツ利用システム。

【請求項20】

前記テーブルは、さらに、該当コンテンツへのアクセス情報を記録し、
前記テーブル手段は、前記テーブルに記録されたコンテンツIDの数が前記しきい値に達したとき、前記アクセス情報に基づいて削除すべきコンテンツIDを決定することを特徴とする請求項18に記載のコンテンツ利用システム。

【請求項21】

前記テーブル手段は、前記テーブルに記録されたコンテンツID数が前記しきい値に達したとき、乱数を生成して当該乱数に基づいて削除すべきコンテンツIDを決定することを特徴とする請求項18に記載のコンテンツ利用システム。

【請求項22】

ネットワーク鍵を共有するコンテンツ取り込み装置と1以上のコンテンツ利用装置とを含み、コンテンツの復号に必要なコンテンツ鍵を含むコンテンツ鍵情報をネットワーク鍵を用いて暗号化することによって、コンテンツをネットワークにバインドするコンテンツ利用システムであって、

前記コンテンツ取り込み装置は、

コンテンツと、当該コンテンツのコンテンツ鍵を含む暗号化コンテンツ鍵情報とを外部から取得する取得手段と、

取得手段により取得されたコンテンツを識別するためのコンテンツIDを生成するID生成手段と、

取得手段により取得された暗号化コンテンツ鍵情報を復号し、復号されたコンテンツ鍵情報にコンテンツIDを付加して、前記ネットワーク鍵を用いて再暗号化することによって暗号変換する暗号変換手段と、

を備え、

前記各コンテンツ利用装置は、

ネットワーク鍵を用いて暗号化されたコンテンツ鍵情報を復号する第1復号手段と、

第1復号手段により復号されたコンテンツ鍵情報中のコンテンツ鍵を用いて前記コンテンツを復号する第2復号手段と、

10

20

30

40

50

第2復号手段によって復号されたコンテンツを蓄積メディアに書き出す書き出し手段と、
第1復号手段により復号されたコンテンツ鍵情報に含まれるコンテンツIDと、当該コンテンツIDに対応するコンテンツが前記書き出し手段によって書き出された回数とを対応させたテーブルを記憶するテーブル記憶手段と、

前記書き出し手段が書き出そうとするコンテンツのコンテンツIDを取得して、前記テーブルから当該コンテンツIDに対応するコンテンツが書き出された回数を参照し、当該回数が予め定められた最大回数に達していれば、書き出し手段による当該コンテンツの書き出しを抑制する抑制手段と

を備える

ことを特徴とするコンテンツ利用システム。

10

【請求項23】

前記コンテンツ利用装置は、さらに、第2復号手段によって復号されたコンテンツを再生する再生手段を有し、

前記抑制手段は、さらに、前記再生手段が再生しようとするコンテンツのコンテンツIDを取得して、前記テーブルから当該コンテンツIDに対応するコンテンツが書き出された回数を参照し、当該回数が前記最大回数に達していれば、再生手段による再生を抑制することを特徴とする請求項22記載のコンテンツ利用システム。

【請求項24】

前記コンテンツ利用装置は、さらに、

前記テーブルを、他のコンテンツ利用装置のテーブルと同期するためのテーブル同期手段を備え、

20

前記テーブル同期手段は、前記テーブルが更新されたとき、前記他のコンテンツ利用装置におけるテーブル同期手段に対し、少なくとも前記コンテンツIDを含む同期情報を送信し、前記他のコンテンツ利用装置におけるテーブル同期手段から同期情報を受信したとき、前記テーブル記憶手段の前記テーブルを更新する

ことを特徴とする請求項22記載のコンテンツ利用システム。

【請求項25】

ネットワーク鍵を共有するコンテンツ取り込み装置と1つ以上のコンテンツ利用装置とを含み、コンテンツの復号に必要なコンテンツ鍵を含むコンテンツ鍵情報をネットワーク鍵を用いて暗号化することによって、コンテンツをネットワークにバインドするコンテンツ利用システムであって、

30

前記各コンテンツ取り込み装置は、

コンテンツと、当該コンテンツのコンテンツ鍵を含む暗号化コンテンツ鍵情報とを外部から取得する取得手段と、

取得されたコンテンツを識別するためのコンテンツIDを生成するID生成手段と、

取得手段により取得された暗号化コンテンツ鍵情報を復号し、復号されたコンテンツ鍵情報にコンテンツIDを付加して、前記ネットワーク鍵を用いて再暗号化することによって暗号変換する暗号変換手段と、

前記コンテンツ利用装置において蓄積メディアに書き出したコンテンツのコンテンツIDを記録するためのテーブルを記憶するテーブル記憶手段と、

40

前記コンテンツ利用装置から書き出し可否判定要求を受けたとき、前記テーブルを用いてコンテンツの書き出し可否判定を行い、書き出し可否判定結果に基づいて前記テーブルを更新するテーブル管理手段と、

前記コンテンツ利用装置から書き出し可否判定要求を受信し、前記テーブル管理手段から取得した書き出し可否判定結果を送信するコンテンツID受信手段と、

を備え、

前記コンテンツ利用装置は、

再暗号化されたコンテンツ鍵情報を前記ネットワーク鍵を用いて復号する第1復号手段と

、
前記コンテンツ取り込み装置に対し、復号されたコンテンツ鍵情報に含まれるコンテンツ

50

I Dを含む書き出し可否判定要求を送信し、書き出し可否判定結果を受信するコンテンツ I D送信手段と、

受信された書き出し可否判定結果が可を示す場合のみ、第1復号手段により復号されたコンテンツ鍵情報に含まれるコンテンツ鍵を用いてコンテンツを復号する第2復号手段と、第2復号手段により復号されたコンテンツを蓄積メディアに書き出す書き出し手段と、を備えることを特徴とするコンテンツ利用システム。

【請求項26】

ネットワーク鍵を共有するコンテンツ取り込み装置と1つ以上のコンテンツ利用装置とを含み、コンテンツの復号に必要なコンテンツ鍵を含むコンテンツ鍵情報をネットワーク鍵を用いて暗号化することによって、コンテンツをネットワークにバインドするコンテンツ利用システムであって、

前記コンテンツ取り込み装置は、

コンテンツと、当該コンテンツのコンテンツ鍵を含む暗号化コンテンツ鍵情報とを外部から取得する取得手段と、

取得されたコンテンツを識別するためのコンテンツ I Dを生成する I D生成手段と、

取得手段により取得された暗号化コンテンツ鍵情報を復号し、復号されたコンテンツ鍵情報にコンテンツ I Dを付加して、前記ネットワーク鍵を用いて再暗号化することによって暗号変換する暗号変換手段と、

前記コンテンツ利用装置において蓄積メディアに書き出したコンテンツのコンテンツ I Dを記録するためのテーブルを記憶する第1テーブル記憶手段と、

前記コンテンツ利用装置から書き出し可否判定要求を受けたとき、前記テーブルを用いてコンテンツの書き出し可否判定を行い、書き出し可否判定結果に基づいて前記テーブルを更新するテーブル管理手段と、

前記コンテンツ利用装置から前記同期情報を受信し、前記テーブルを前記コンテンツ利用装置に送信するテーブル送信手段と、

を備え、

前記コンテンツ利用装置は、

再暗号化された前記コンテンツ鍵情報を前記ネットワーク上で予め共有されている暗号鍵を用いて復号し、前記コンテンツ鍵を出力する第1復号手段と、

前記コンテンツ取り込み装置に対し、少なくともコンテンツ I Dを含む前記テーブルの同期情報を送信し、前記テーブルを受信するテーブル受信手段と、

前記テーブルを記憶する第2テーブル記憶手段と、

前記コンテンツ取り込み装置から受信した前記テーブルで、前記第2テーブル記憶手段のテーブルを更新し、前記テーブルを用いてコンテンツの書き出し可否判定を行うテーブル管理手段と、

テーブル管理手段による判定結果が可を示す場合のみ、暗号化された前記コンテンツを前記コンテンツ鍵で復号する第2復号手段と、

第2復号手段により復号されたコンテンツを蓄積メディアに書き出す書き出し手段とを備えることを特徴とするコンテンツ利用システム。

【請求項27】

ネットワーク鍵を共有するコンテンツ取り込み装置と1つ以上のコンテンツ利用装置と前記コンテンツ利用装置に接続され蓄積メディアにコンテンツを書き出すコンテンツ書き出し装置とを含み、コンテンツの復号に必要なコンテンツ鍵を含むコンテンツ鍵情報をネットワーク鍵を用いて暗号化することによって、コンテンツをネットワークにバインドするコンテンツ利用システムであって、

前記コンテンツ取り込み装置は、

コンテンツと、当該コンテンツのコンテンツ鍵を含む暗号化コンテンツ鍵情報とを外部から取得する取得手段と、

取得されたコンテンツを識別するためのコンテンツ I Dを生成する I D生成手段と、

取得手段により取得された暗号化コンテンツ鍵情報を復号し、復号されたコンテンツ鍵情報

10

20

30

40

50

報にコンテンツIDを付加して、前記ネットワーク鍵を用いて再暗号化することによって暗号変換する暗号変換手段と

を備え、

前記コンテンツ利用装置は、

ネットワーク鍵を用いて再暗号化されたコンテンツ鍵情報を復号する第1復号手段と、

復号されたコンテンツ鍵情報に含まれるコンテンツ鍵で前記コンテンツを復号する第2復号手段と

を備え、

前記コンテンツ書き出し部は、

蓄積メディアにコンテンツを書き出す書き出し手段と、

コンテンツ書き出し手段から蓄積メディアに書き出したコンテンツのコンテンツIDを記録するための、テーブルを記憶するテーブル記憶手段と、

前記テーブルを用いてコンテンツの書き出し可否判定を行い、判定結果に従って書き出し手段を制御するテーブル管理手段と

を備えることを特徴とするコンテンツ利用システム。

【請求項28】

前記第1復号手段は、任意の単位で単調増加または単調減少するIDを生成して、前記IDを前記第2復号手段に送信し、

前記第2復号手段は、受信した前記IDを記録し、書き出し処理を再開する場合に、前記IDを前記第1復号手段に送信し、

前記第1復号手段は、受信した前記IDと最後に生成した前記IDとを比較して、差分がある値以下である場合にのみ、書き出し処理の再開を許可する

ことを特徴とする請求項22記載のコンテンツ利用システム。

【請求項29】

コンテンツ取り込み装置と、1以上の前記コンテンツ利用装置とがネットワーク接続されるコンテンツ利用システムであって、

前記コンテンツ取り込み装置は、

暗号化された前記コンテンツ鍵情報を復号し、前記コンテンツ鍵に作用させるための秘密情報を生成し、前記ネットワークで予め共有された暗号鍵と、前記秘密情報とを用いて前記コンテンツ鍵情報を再暗号化する暗号変換手段と、

前記コンテンツ利用装置から、コンテンツの出力要求を受信し、少なくとも前記秘密情報を含む要求応答を送信する出力要求処理手段と、

を備え、

前記コンテンツ利用装置は、

前記コンテンツ取り込み装置に対し、少なくともコンテンツの出力先を含む出力要求を送信し、要求応答を受信して前記秘密情報を取得する出力要求手段と、

前記ネットワークで予め共有された暗号鍵と、前記秘密情報とを用いて、再暗号化された前記コンテンツ鍵情報を復号する第1復号手段と、

選択手段を制御するためのコンテンツ出力制御情報を出力する制御手段と、

暗号化された前記コンテンツを前記コンテンツ鍵で復号する第2復号手段と、

前記コンテンツ出力制御情報に基づき、前記コンテンツの出力先を選択する選択手段と、

前記コンテンツを出力するための1以上の出力手段と

を備えることを特徴とするコンテンツ利用システム。

【請求項30】

コンテンツの復号に必要なコンテンツ鍵を含むコンテンツ鍵情報をネットワーク鍵を用いて暗号化することによってネットワークにバインドされたコンテンツを利用するコンテンツ利用装置であって、

ネットワーク鍵を用いて再暗号化されたコンテンツ鍵情報を復号する第1復号手段と、

第1復号手段により復号されたコンテンツ鍵情報中のコンテンツ鍵を用いて前記コンテンツを復号する第2復号手段と、

10

20

30

40

50

第2復号手段によって復号されたコンテンツを蓄積メディアに書き出す書き出し手段と、
第1復号手段により復号されたコンテンツ鍵情報に含まれるコンテンツIDと、当該コンテンツIDに対応するコンテンツが前記書き出し手段によって書き出された回数とを対応させたテーブルを記憶するテーブル記憶手段と、

前記書き出し手段が書き出そうとするコンテンツのコンテンツIDを取得して、前記テーブルから当該コンテンツIDに対応するコンテンツが書き出された回数を参照し、当該回数が予め定められた最大回数に達していれば、書き出し手段による当該コンテンツの書き出しを抑制する抑制手段と

を備えることを特徴とするコンテンツ利用装置。

【請求項31】

ネットワーク鍵を共有する複数の装置が接続されてネットワークにおいて、コンテンツの復号に必要なコンテンツ鍵を含むコンテンツ鍵情報をネットワーク鍵を用いて暗号化することによって、コンテンツをネットワークにバインドするコンテンツ取り込み装置であって、

コンテンツと、当該コンテンツのコンテンツ鍵を含む暗号化コンテンツ鍵情報とを外部から取得する取得手段と、

取得手段により取得されたコンテンツを識別するためのコンテンツIDを生成するID生成手段と、

取得手段により取得された暗号化コンテンツ鍵情報を復号し、復号されたコンテンツ鍵情報にコンテンツIDを付加して、前記ネットワーク鍵を用いて再暗号化することによって暗号変換する暗号変換手段と、

を備え、

前記コンテンツIDは、ネットワークにバインドされたコンテンツを、バインドされていない状態で蓄積メディアに書き出すことを管理するために用いられることを特徴とするコンテンツ取り込み装置。

【請求項32】

複数の装置が接続されたネットワークにおいてコンテンツを利用するコンテンツ利用方法であって、

前記複数の装置のうち少なくとも1つの装置において、コンテンツをネットワーク上の装置のみが利用可能な状態にすることによってコンテンツをネットワークにバインドするバインドステップと、

前記複数の装置のうち少なくとも1つの装置において、前記バインドステップにおいてバインドされたコンテンツに対応させてコンテンツIDを発行するID発行ステップと、

前記複数の装置のうち少なくとも1つの装置において、ネットワークにバインドされたコンテンツをバインドされていない状態にしてこれから書き出そうとするコンテンツのコンテンツIDを取得して、既に書き出されたコンテンツのIDを記録したテーブルをメモリから参照して、書き出し可否を判定する判定ステップと、

前記複数の装置のうち少なくとも1つの装置において、判定ステップにおいて書き出し可と判定された場合に、前記バインドステップにおいてバインドされたコンテンツについて、バインドされた状態を解除するバインド解除ステップと、

前記複数の装置のうち少なくとも1つの装置において、バインド解除ステップにおいてバインドを解除されたコンテンツを蓄積メディアに書き出す書き出しステップと、
を有することを特徴とするコンテンツ利用方法。

【請求項33】

コンテンツの復号に必要なコンテンツ鍵を含むコンテンツ鍵情報をネットワーク鍵を用いて暗号化することによってネットワークにバインドされたコンテンツを利用する装置におけるコンテンツ利用方法であって、

ネットワーク鍵を用いて再暗号化されたコンテンツ鍵情報を復号する第1復号ステップと、

第1復号ステップにおいて復号されたコンテンツ鍵情報中のコンテンツ鍵を用いて前記コ

10

20

30

40

50

ンテンツを復号する第2復号ステップと、

ネットワークにバインドされたコンテンツをバインドされていない状態にしてこれから書き出そうとするコンテンツのコンテンツIDを取得して、既に書き出されたコンテンツのIDを記録したテーブルをメモリから参照して、書き出し可否を判定する判定ステップと、

判定ステップにおいて書き出し可と判定された場合に、前記バインドされたコンテンツについて、バインドされた状態を解除してバインドされていない状態で蓄積メディアに書き出す書き出しステップと、

を有することを特徴とするコンテンツ利用方法。

【請求項34】

ネットワーク鍵を共有するコンテンツ取り込み装置と1以上のコンテンツ利用装置とを含み、コンテンツの復号に必要なコンテンツ鍵を含むコンテンツ鍵情報をネットワーク鍵を用いて暗号化することによって、コンテンツをネットワークにバインドするコンテンツ利用システムにおいて、コンテンツ取り込み装置において実行される第1プログラムと、コンテンツ利用装置において実行される第2プログラムとからなるコンテンツ利用プログラムであって、

前記第1プログラムは、

コンテンツと、当該コンテンツのコンテンツ鍵を含む暗号化コンテンツ鍵情報とを外部から取得する取得手段と、

取得手段により取得されたコンテンツを識別するためのコンテンツIDを生成するID生成手段と、

取得手段により取得された暗号化コンテンツ鍵情報を復号し、復号されたコンテンツ鍵情報にコンテンツIDを付加して、前記ネットワーク鍵を用いて再暗号化することによって暗号変換する暗号変換手段と

を含む各手段をコンピュータに機能させ、

前記第2プログラムは、

ネットワーク鍵を用いて再暗号化されたコンテンツ鍵情報を復号する第1復号手段と、

第1復号手段により復号されたコンテンツ鍵情報中のコンテンツ鍵を用いて前記コンテンツを復号する第2復号手段と、

第2復号手段によって復号されたコンテンツを蓄積メディアに書き出す書き出し手段と、

第1復号手段により復号されたコンテンツ鍵情報に含まれるコンテンツIDと、当該コンテンツIDに対応するコンテンツが前記書き出し手段によって書き出された回数とを対応させたテーブルを記憶するテーブル記憶手段と、

前記書き出し手段が書き出そうとするコンテンツのコンテンツIDを取得して、前記テーブルから当該コンテンツIDに対応するコンテンツが書き出された回数を参照し、当該回数が予め定められた最大回数に達していれば、書き出し手段による当該コンテンツの書き出しを抑制する抑制手段と

を含む各手段をコンピュータに機能させる

ことを特徴とするコンテンツ利用プログラム。

【請求項35】

コンテンツの復号に必要なコンテンツ鍵を含むコンテンツ鍵情報をネットワーク鍵を用いて暗号化することによってネットワークにバインドされたコンテンツを利用する装置において実行されるコンテンツ利用プログラムであって、

前記プログラムは、

ネットワーク鍵を用いて再暗号化されたコンテンツ鍵情報を復号する第1復号手段と、

第1復号手段により復号されたコンテンツ鍵情報中のコンテンツ鍵を用いて前記コンテンツを復号する第2復号手段と、

第2復号手段によって復号されたコンテンツを蓄積メディアに書き出す書き出し手段と、

第1復号手段により復号されたコンテンツ鍵情報に含まれるコンテンツIDと、当該コンテンツIDに対応するコンテンツが前記書き出し手段によって書き出された回数とを対応

10

20

30

40

50

ませたテーブルを記憶するテーブル記憶手段と、
前記書き出し手段が書き出そうとするコンテンツのコンテンツIDを取得して、前記テーブルから当該コンテンツIDに対応するコンテンツが書き出された回数参照し、当該回数が予め定められた最大回数に達していれば、書き出し手段による当該コンテンツの書き出しを抑制する抑制手段と
を含む各手段をコンピュータに機能させる
ことを特徴とするコンテンツ利用プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、通信や放送などで配信された映像や音声などのデジタルコンテンツを利用するシステムに関し、特に、コンテンツを外部蓄積メディアに書き出す場合のコンテンツの利用制御に関する。

【0002】

【従来の技術】

近年、音楽や映像、ゲームなどのデジタルコンテンツをインターネットやデジタル放送で配信し、利用するシステムが実用化の段階を迎えている。

【0003】

従来のコンテンツ利用システムでは、特許文献1～3に見られるように、放送で配信されたコンテンツをネットワークにバインドすることにより、コンテンツをネットワーク内で共有し、利用することができる。ここで、コンテンツをネットワークにバインドするというのは、ネットワーク内の正当な端末のみが当該コンテンツを利用できる状態にすることをいう。言い換えれば、正当でない他の端末がネットワークに接続されても、当該他の端末が当該コンテンツを利用できない状態にすることをいう。あるいは、ネットワークにバインドされたコンテンツを他のネットワークに移動させた場合も、他のネットワークの端末が当該コンテンツを利用できない状態にすることをいう。

【0004】

例えば、暗号化されて配信されたコンテンツをネットワーク（例えば、家庭内ネットワーク）に取り込む場合、暗号化されたコンテンツは変換せずそのままネットワーク内の端末が利用し、コンテンツの暗号鍵を暗号変換することによって、コンテンツをネットワークにバインドすることができる。ここで暗号変換は、暗号鍵を一旦復号した上で、さらにネットワーク上で予め共有されている暗号鍵（以下、ネットワーク鍵と記す）を用いて、コンテンツの暗号鍵を再暗号化することをいう。

【0005】

ネットワークにバインドされたコンテンツを利用する場合、ネットワーク鍵を保持しているネットワーク上の機器は、共有しているネットワーク鍵を用いてコンテンツの再暗号化された暗号鍵を復号することができるので、復号された暗号鍵を用いて暗号化されたコンテンツを復号することができる。

【0006】

一方、ネットワーク鍵を保持していない機器は、コンテンツの暗号鍵を復号することができないため、暗号化されたコンテンツも復号することができないようになっている。

【0007】

下記特許文献1～3等の従来のコンテンツ利用システムでは、ネットワークにコンテンツをバインドすると、ハードディスク等のネットワーク上の蓄積媒体にコンテンツとコンテンツ暗号鍵のコピーをネットワークにバインドされた状態で作成することが無制限に可能であるが、その利用（再生等）に関しては、ネットワーク機器の数を制限することによって、制限を課するようになっている。

【0008】

【特許文献1】

特開平11-331805号公報

10

20

30

40

【0009】

【特許文献2】

米国特許公報5878135号明細書

【0010】

【特許文献3】

米国特許公報6016348号明細書

【0011】

【発明が解決しようとする課題】

ところで、上記従来技術によれば、ネットワークにバインドされていない状態でコンテンツをネットワーク外に書き出すことが実際できないようになっている。これに対して、ネットワークにバインドされたコンテンツをDVD-RAM、D-VHS、SDカード等のメモ리카ードといった外部蓄積メディアに書き出して(MOVE、EXPORT等)コンテンツを利用したいといったユーザの要求がある。

10

【0012】

このように、従来のコンテンツ利用システムでは、バインドされていない状態で書き出すことは考慮されておらず、上記のようなユーザの要求を満たすことができないという問題がある。

【0013】

また、仮に、コンテンツをバインドしていない状態で書き出すことが可能であると仮定しても、蓄積メディアへのコンテンツのコピーが無制限に作成できてしまう恐れがあり、コンテンツの著作権保護の観点から問題が生ずることになる。

20

【0014】

本発明は、こうした従来の問題点に鑑み、ネットワークにバインドされたコンテンツについて、上記のユーザ要求と著作権保護という相対立する要求をバランス良く解決するコンテンツ利用システムを提供することを目的とする。

【0015】

言い換えれば、ネットワークにバインドされたコンテンツを蓄積メディアに書き出したいというユーザ要求を満たしながら十分な著作権保護を可能にするコンテンツ利用システムを提供することを目的とする。

【0016】

【課題を解決するための手段】

上記目的を達成するために、本発明におけるコンテンツ利用システムは、複数の装置が接続されたネットワークにおいてコンテンツを利用するコンテンツ利用システムであって、前記複数の装置のうち少なくとも1つの装置に備えられ、コンテンツをネットワーク上の装置のみが利用可能な状態にすることによってコンテンツをネットワークにバインドするバインド手段と、前記複数の装置のうち少なくとも1つの装置に備えられ、前記バインド手段によってバインドされたコンテンツに対応させてコンテンツIDを発行するID発行手段と、前記複数の装置のうち少なくとも1つの装置に備えられ、前記バインド手段によってバインドされたコンテンツについて、バインドされた状態を解除するバインド解除手段と、前記複数の装置のうち少なくとも1つの装置に備えられ、前記バインド解除手段によってバインドを解除されたコンテンツを蓄積メディアに書き出す書き出し手段と、前記複数の装置のうち少なくとも1つの装置に備えられ、書き出し手段により書き出されたコンテンツのコンテンツIDを示すテーブルを記憶するテーブル手段と、前記複数の装置のうち少なくとも1つの装置に備えられ、書き出し手段が書き出そうとするコンテンツのコンテンツIDを取得して、前記テーブルの内容に基づいて書き出し手段による当該コンテンツの書き出しを抑制する抑制手段とを備える。

30

40

【0017】

この構成によれば、ネットワークにバインドされたコンテンツ毎に、コンテンツIDを付与して、コンテンツの書き出しテーブルによって管理するので、書き出し手段によって無制限に書き出しすることを抑制することができる。つまり、ネットワークにバインドされ

50

ていない状態で書き出すことを制限することができる。例えば、家庭内のネットワークにバインドされたコンテンツを蓄積メディアに書き出したいという個人ユーザの要求を満たしながらも著作権を十分に保護することができるので、ユーザの私的利用と著作権者との間の相対立する利益をバランスよく満たすことができる。

【0018】

ここで、前記抑制手段は、書き出し手段が書き出そうとするコンテンツのコンテンツIDを取得し、前記テーブルに当該コンテンツIDが既に記録されていなければ、前記書き出し手段に対して当該コンテンツの書き出しを抑制しないで前記テーブルに取得したコンテンツIDを追加し、前記テーブルに当該コンテンツIDが既に存在していれば、前記書き出し手段に対して当該コンテンツの書き出しを抑制する構成としてもよい。

【0019】

この構成によれば、抑制手段は前記テーブルに当該コンテンツIDが既に存在していれば、前記書き出し手段に対して当該コンテンツの書き出しを抑制するので、書き出し手段による書き出しをコンテンツ毎に1回許可し、2回目以降を禁止することができる。

【0020】

ここで、前記抑制手段は、書き出し手段が書き出そうとするコンテンツのコンテンツIDを取得して、前記テーブルに当該コンテンツIDが存在していなければ、当該コンテンツID及び、書き出し手段による書き出し回数を1として追加し、前記テーブルに当該コンテンツIDが存在し、かつ書き出し回数が予め定められた最大回数に達していれば、書き出し手段による書き出しを抑制する構成としてもよい。

【0021】

この構成によれば、抑制手段は、前記テーブルに当該コンテンツIDが存在し、かつ書き出し回数が予め定められた最大回数に達していれば、書き出し手段による書き出しを抑制するので、書き出し手段による書き出しをコンテンツ毎に最大回数の範囲内で許可し、それを超える場合は禁止することができる。最大回数は1つの値を予め決めておいてもよいし、コンテンツ毎に予め決めておいてもよいので、ユーザと著作権者との相対立する利益をより柔軟にバランスをとることができる。

【0022】

ここで、前記バインド手段は、前記複数の装置に共有されているネットワーク鍵を用いて、コンテンツの復号するためのコンテンツ鍵を暗号化することによって、コンテンツをネットワークにバインドする構成としてもよい。

【0023】

この構成によれば、コンテンツそのものをネットワーク鍵で暗号化する必要はないので、バインドするための処理負荷を小さくすることができる。

ここで、前記複数の装置は、1つのコンテンツ取り込み装置と、少なくとも1つのコンテンツ利用装置とを含み、前記コンテンツ取り込み装置は前記バインド手段と前記ID発行手段とを備え、前記各コンテンツ利用装置は前記テーブル手段と前記バインド解除手段と前記書き出し手段と抑制手段とを備える構成としてもよい。

【0024】

この構成によれば、コンテンツのバインド及びコンテンツIDの生成は、ネットワーク上に1つ存在するコンテンツ取り込み装置において集中して処理することができる。

【0025】

ここで、前記コンテンツ利用装置は、さらに、書き込み手段により書き込みを行った際に少なくとも当該コンテンツIDを他のコンテンツ利用装置に通知する通知手段と、他のコンテンツ利用装置から通知を受けたときに前記テーブル手段に記憶されたテーブルを更新する更新手段とを備える構成としてもよい。

【0026】

この構成によれば、ネットワーク上の複数のコンテンツ利用装置の間でテーブルの内容を容易に一致させることができる。

ここで、前記コンテンツ利用システムは、1つのコンテンツ取り込み装置と、少なくとも

10

20

30

40

50

1つのコンテンツ利用装置とを含み、前記コンテンツ取り込み装置は、前記バインド手段と、前記ID発行手段と、前記テーブル手段と、前記抑制手段とを備え、前記各コンテンツ利用装置は、前記バインド解除手段と前記書き出し手段とを備える構成としてもよい。

【0027】

この構成によれば、コンテンツのバインドと、コンテンツIDの生成と、テーブルの管理と、書き出しの抑制とを、ネットワーク上に1つ存在するコンテンツ取り込み装置において集中して処理することができる。各コンテンツ利用手段は、コンテンツ取り込み装置における抑制手段に従って書き出しを行えばよいので、テーブルを個別に管理する負荷がからない。

【0028】

また、本発明のコンテンツ利用方法及びコンテンツ利用プログラムについても上記と同様の構成、作用及び効果を有する。

【0029】

【発明の実施の形態】

(実施の形態1)

以下、本発明の実施の形態1について、図面を用いて詳細に説明する。

【0030】

図1は、本発明の実施の形態1に関わるコンテンツ利用システム1の全体の構成を示す図である。

このコンテンツ利用システムは、デジタル放送で配信されるコンテンツを、ネットワークで接続された機器で利用するシステムであり、コンテンツを取り込むためのコンテンツ取り込み装置100と、記憶装置90と、コンテンツを利用する複数のコンテンツ利用装置110-1、110-2、110-3等と、これらを接続するネットワーク120とから構成される。

【0031】

コンテンツ取り込み装置100は、放送波からコンテンツを取り込み、少なくともコンテンツの暗号鍵（以下、コンテンツ鍵と記す）を含む、暗号化されたコンテンツ鍵情報を復号し、ネットワークで予め共有された暗号鍵（以下、ネットワーク鍵と記す）を用いてコンテンツ鍵情報を再暗号化、すなわち暗号変換することにより、コンテンツをネットワークにバインドする。

【0032】

例えば、コンテンツ取り込み装置100は、図2に示すように、デジタル放送を受信するためのSTB（Set Top Box）であり、CAS（Conditional Access System）でアクセス制御されたコンテンツと、アクセス鍵情報としてコンテンツ鍵を含む暗号化されたECM（Element Control Message）とを受信し、ECMセクションを再構成して、暗号化されたECMの暗号を一旦復号し、ネットワーク鍵で再暗号化して、ネットワーク120にコンテンツと再暗号化したECMを流す、といった処理を行う。なお、ECMは、MPEG-2 Systemで規定されたPrivateセクションで実現され、図4で示されるような構造となっている。なお、MPEG-2 Systemは、国際標準であるISO/IEC 13818-1に規定されている。

【0033】

図4に示したECMセクションは、セクションヘッダとECM本体とセクションテラ（誤り検出符号）を有する構成となっている。同図のECMセクションには、ECM本体の内容の一例として、バージョン番号、コピー制御情報、コンテンツ鍵、可変長のフライベートデータ、改ざん検出用データとが示されている。バージョン番号はECMのバージョンを示す。コピー制御情報は、コンテンツのコピーの許否（COPY FREE、NETWORK COPY、COPY NEVER等）を示す。コンテンツ鍵は、スクランブル鍵とも呼ばれ、コンテンツの暗号化及び復号化用である。フライベートデータは、可変長の任意データが挿入される。改ざん検出用データはECMの改ざんを検出するために設定

10

20

30

40

50

される。なお、ECMの暗号化部分はECM本体全体であり、EMM(Entitlement Management Message)で配信されるワーク鍵等で暗号化される。

【0034】

上記のコピー制御情報は、著作者又はコンテンツプロバイダ/サービスプロバイダ等によって設定される。COPY NEVERは、コピー不可であって、視聴のみ可能であることを意味し、ネットワークにバインドされない。NETWORK COPYは、プライベートネットワーク内でのみ自由にコピー可能であることを意味し、ネットワークにバインドされる。COPY FREEは、自由にコピー可能であることを意味し、ネットワークにバインドされてもよいが、その必要はない。

【0035】

また、本実施の形態では、コンテンツプロバイダ/サービスプロバイダは、上記のプライベートデータ内に、最大書き出し回数、書き出し先、書き出し経路等を設定することができ、これは、ネットワークにバインドされたコンテンツの書き出し及び再生表示を制御するための条件として用いられる。

【0036】

記憶装置90は、コンテンツ取り込み装置100によって取り込まれたコンテンツ及び暗号変換されたコンテンツ鍵情報を記憶する。つまり、記憶装置90は、ネットワークにバインドされた状態のコンテンツを記憶する。

【0037】

例えば、記憶装置90は、図2に示すようなホームサーバであり、ハードディスクを備え、ネットワーク上の装置からアクセス可能になっている。

コンテンツ利用装置110-1、110-2、110-3等は、コンテンツ取り込み装置100又は記憶装置90から、コンテンツおよび暗号変換されたコンテンツ鍵情報を取得し、既に取得済みのネットワーク鍵を用いて、暗号化されたコンテンツ鍵情報を復号してコンテンツ鍵を取り出し、コンテンツ鍵でコンテンツを復号してコンテンツを利用する。また、本コンテンツ利用システム1では、複数のコンテンツ利用装置110-1、110-2、110-3等をネットワーク120に接続することができる。

【0038】

例えば、コンテンツ利用装置110-1、110-2、110-3等は、図2に示すように、デジタルTV110-1、D-VHS110-2、DVDレコーダ110-3、PC110-4などであり、コンテンツの表示、取り外し可能な蓄積メディア(D-VHSテープ、DVD-RAM、SDメモリーカード等)への記憶を行う機器である。あるいは、コンテンツ利用装置110は、これらの機能を複合した機器である。

【0039】

ネットワーク120は、コンテンツ取り込み装置100およびコンテンツ利用装置110-1、110-2、110-3等を相互に接続するネットワークであり、例えば、IEEE1394バス、IEEE802.3(10/100Base-T)、Bluetoothなどで実現される。

【0040】

図3は、図1に示されるコンテンツ取り込み装置100およびコンテンツ利用装置110の構成を示す機能ブロック図である。このコンテンツ利用システムは、ネットワークにバインドされたコンテンツをコンテンツ毎に識別できるようにし、当該コンテンツをネットワークにバインドしていない状態でコンテンツの書き出すことに制限を課するように構成されている。なお、コンテンツ利用装置110は、同等の構成を有するコンテンツ利用装置110-1、110-2、110-3等の1つの代表として図示している。また、本図には、記憶装置90及びネットワーク120も併せて示されている。

【0041】

コンテンツ取り込み装置100は、入力部101と、分離部102と、コンテンツ鍵情報暗号変換部103と、コンテンツID生成部104と、多重化部105とを備えている。

10

20

30

40

50

【0042】

入力部101は、デジタル放送のMPEG-2トランスポートストリーム(TS)を入力ストリームとして取り込む。トランスポートストリームは、コンテンツ、ECM、EMM、PSI(Program Specific Information)などがパケット多重された構成となっており、トランスポートストリームパケット(TSパケット)のヘッダ部のPID(Packet ID)で識別できるようになっている。

【0043】

分離部102は、入力部101で取り込んだトランスポートストリームをコンテンツ、ECM等に分離する。

具体的には、PMT(Program Map Table)と呼ばれるPSIを参照して、ストリームを構成するエレメンタリのPIDを取得する。そして、TSパケットのヘッダ部のPIDを参照し、コンテンツ、ECM等のパケットを分離する処理を行う。

【0044】

コンテンツ鍵情報暗号変換部103は、分離部102から受信したECMのパケットからECMセクションを再構成し、ECMを取り出し、当該ECMを暗号変換する。つまり暗号化されたECMを一旦復号して前述のネットワーク鍵を用いて復号されたECMを再暗号化する。

【0045】

具体的には、ECMは、CASのワーク鍵で暗号化されて放送波に多重された状態で配信される。コンテンツ鍵情報暗号変換部103は、CASのワーク鍵で暗号化されたECMを復号し、コンテンツID生成部104にコンテンツIDの発行を要求し、要求に応じてコンテンツID生成部104で生成されたコンテンツIDを復号したECMに挿入した上で、ネットワーク鍵を用いて再度ECMを暗号化する。なお、ワーク鍵は、コンテンツの配信に先立ち、EMMによって放送波に多重されて配信されているのが一般的であるので、コンテンツ鍵情報暗号変換部103は、予めワーク鍵を取得することができる。

【0046】

このように、コンテンツの暗号鍵であるコンテンツ鍵を含むECMにコンテンツIDを挿入することにより、コンテンツとコンテンツIDをセキュアにバインドしている。ここで、コンテンツIDを付与する単位は、分離部102によって識別されるイベントの単位でよい。ここでイベントは1つの放送番組に相当するコンテンツをいう。この場合、コンテンツ鍵情報暗号変換部103は、TS中のSI(Service Information)のEIT(Event Information Table)からevent-id等のイベント情報を取得することによってイベントを識別し、このイベント単位でコンテンツIDの生成を要求する。

【0047】

コンテンツID生成部104は、コンテンツ鍵情報暗号変換部103からの要求に基づき、ユニークなコンテンツIDを発行する。具体的には、コンテンツID生成部104は、内部にカウンタを有し、コンテンツ鍵情報暗号変換部103からコンテンツID発行の要求を受ける度に現在のカウンタ値をコンテンツIDに割り当て、カウンタをインクリメントするといった処理を行う。

【0048】

多重化部105は、分離部102から受け取ったコンテンツと、コンテンツ鍵情報暗号変換部103から受け取った暗号化されたECMとを、再度トランスポートストリームとして多重化する処理を行う。

【0049】

記憶装置90は、多重化部105から出力されるトランスポートストリームを記憶する。一方、コンテンツ利用装置110は、分離部111と、コンテンツ鍵情報復号部112と、書き出しコンテンツリスト管理部113と、書き出しコンテンツリスト蓄積部114と、コンテンツ出力制御部115と、コンテンツ復号部116と、コンテンツ出力選択部117と、コンテンツ出力部としてコンテンツ表示部118およびコンテンツ書き出し部1

10

20

30

40

50

１９とを揃える。

【００５０】

分離部１１１は、コンテンツ利用装置１１０においてユーザからコンテンツ表示要求又はコンテンツ書き出し要求を受けた場合に、コンテンツ取り込み装置１００又は記憶装置９０から取得したトランスポートストリームからコンテンツと再暗号化ＥＣＭとを分離する。

【００５１】

コンテンツ鍵情報復号部１１２は、分離部１１１から再暗号化ＥＣＭを受信し、ネットワーク鍵を用いて再暗号化されたＥＣＭを復号する。その際、ユーザからのコンテンツ書き出し要求があった場合には、書き出しコンテンツリスト管理部１１３による書き出しについての判定結果が許可である場合にのみ、復号したコンテンツ鍵をコンテンツ復号部１１６に渡す。具体的には、コンテンツ鍵情報復号部１１２は、ネットワーク鍵を用いて再暗号化されたＥＣＭを復号し、そのＥＣＭに含まれるコンテンツＩＤを書き出しコンテンツリスト管理部１１３に渡し、該当コンテンツＩＤのコンテンツの書き出しを許可するか禁止するかを示す判定結果を受け取り、判定結果が許可である場合に、復号したコンテンツ鍵をコンテンツ復号部１１６に渡す。このように、コンテンツリスト管理部１１３において個々のコンテンツについて書き出しの許可を判定することにより、コンテンツをバインドしていない状態で無制限に外部に出力することができないようにしている。

【００５２】

また、ユーザからのコンテンツ表示要求があった場合のコンテンツ鍵情報復号部１１２の処理も、コンテンツ書き出し要求があった場合と同様である。ただし、書き出しコンテンツリスト管理部１１３から得られる判定結果は書き出しの許可又は禁止についての判定結果ではなくコンテンツの再生表示についての判定結果である。

【００５３】

書き出しコンテンツリスト管理部１１３は、書き出しコンテンツリスト蓄積部１１４に蓄積された書き出しコンテンツリスト（Moved Content List、以下、MCLと記す）に基づいてコンテンツ出力を許可するか禁止するかを判定し、MCLの更新を行う。ここで、MCLは、少なくとも既に書き出しがなされたコンテンツのコンテンツＩＤを含むリストである。コンテンツ出力許可判定は、コンテンツの書き出しの許可の判定と、コンテンツ再生表示の許可の判定とがある。

【００５４】

具体的には、書き出しコンテンツリスト管理部１１３は、コンテンツＩＤをコンテンツ鍵情報復号部１１２から受け取った場合、次の（Ａ）又は（Ｂ）等の処理によりコンテンツの書き出し許可の判定を行う。

【００５５】

（Ａ）受け取ったコンテンツＩＤが既にMCLに登録されているか否かを判定し、登録されていない場合は、MCLに当該コンテンツＩＤを追加して書き出しを許可し、既に登録されている場合は、コンテンツの書き出しを禁止する。この場合、各コンテンツに対して書き出しを１回だけ許可し、２回目以降は禁止することができる。この場合のMCLは、既に１回書き出したコンテンツのコンテンツＩＤリストとなる。MCLにコンテンツＩＤが登録されていないことが、コンテンツを書き出すための条件（書き出し条件）となる。

【００５６】

（Ｂ）受け取ったコンテンツＩＤが既にMCLに登録されているか否かを判定し、登録されていない場合は、MCLに当該コンテンツＩＤを登録し、予め定められた書き出し条件又はMCLに従ってコンテンツ書き出しの許可を判定し、登録されている場合は、当該コンテンツＩＤに対応する書き出し条件に従ってコンテンツの書き出しの許可を判定する。ここで、書き出し条件は、例えば、コンテンツの書き出し可能回数、書き出し先（どの蓄積メディアに書き出せるか）、書き出し経路（アナログ出力／デジタル出力など）等であり、この場合、コンテンツ毎に、書き出し条件に従ってコンテンツの書き出しを制限することになる。コンテンツの書き出し可能回数は、例えばネットワーク１２０内でネットワーク鍵

10

20

30

40

50

を共有しているコンテンツ利用装置 110 の数である。

【0057】

また、コンテンツリスト管理部 113 は、コンテンツの再生表示についての拒否の判定についても上記 (A) (B) と同様に判定するが、コンテンツの書き出し条件ではなくコンテンツの再生表示条件に従う。

【0058】

また、書き出しコンテンツリスト管理部 113 は、書き出しコンテンツリスト蓄積部 114 の MCL のハッシュ値をセキュアに管理する。これは、MCL をハードディスク等の非セキュアな領域に蓄積する場合に、不正なユーザによる改ざんの有無の検出を行い、その正当性を確保するためである。そのため書き出しコンテンツリスト管理部 113 は、MCL の内容が更新される度に、MCL のハッシュ値を計算し、計算結果を管理する。ハッシュ値のセキュアな管理方法の一例としては、ハード的に耐タンパ化されたセキュリティモジュールの内部にハッシュ値を格納する方法が挙げられる。

【0059】

さらに、書き出しコンテンツリスト管理部 113 は、MCL の最大サイズ、あるいは、コンテンツ ID 数や MCL のサイズに関するしきい値を管理する。これは、MCL に掲載する最大コンテンツ ID 数や最大バイト数などのしきい値を管理しておき、MCL がしきい値に達した場合は、MCL への掲載の古いコンテンツ ID の情報から削除する処理を行う。具体的には、書き出しコンテンツリスト管理部 113 は、次に MCL へ書き込む位置を示すポインタを管理し、MCL が上限値に達した場合は、ポインタを MCL の先頭に戻すことにより、古いコンテンツ ID の情報から削除することが可能となる。

【0060】

あるいは、コンテンツへのアクセス日時を MCL のコンテンツ毎の情報として書き込んでおくことにより、アクセス頻度の少ない情報から削除（上書き）するようにすることもできる。

【0061】

あるいは、上述のように自動的に削除するのではなく、MCL から削除する情報をユーザに選択させ、ユーザ操作により削除するようにしても良い。

書き出しコンテンツリスト蓄積部 114 は、MCL を蓄積しておく部であり、ハードディスク等によって実現される。

【0062】

コンテンツ出力制御部 115 は、コンテンツ出力選択部 117 に対し、コンテンツ出力を制御するためのコンテンツ出力制御情報を出力する。具体的には、コンテンツ出力制御部 115 は、ユーザからのコンテンツ表示要求または書き出し要求に基づき、コンテンツをコンテンツ表示部 118 に出力するか、コンテンツ書き出し部 119 に出力するかを指定するためのコンテンツ出力制御情報を生成し、コンテンツ出力選択部 117 に送信する。

【0063】

コンテンツ復号部 116 は、暗号化されたコンテンツを復号する。具体的には、コンテンツ鍵により暗号化されているコンテンツの TS パケットを、コンテンツ鍵情報復号部 112 から取得したコンテンツ鍵を用いて、順次復号する処理を行う。

【0064】

コンテンツ出力選択部 117 は、コンテンツ出力制御部 115 から取得したコンテンツ出力制御情報に基づき、コンテンツの渡し先を制御する。具体的には、コンテンツ出力制御情報が表示を示す場合は、コンテンツをコンテンツ表示部 118 に送信し、コンテンツ出力制御情報が蓄積メディアへの書き出しを示す場合は、コンテンツをコンテンツ書き出し部 119 に送信する処理を行う。

【0065】

コンテンツ表示部 118 は、コンテンツの TS パケットから MPEG-2 のエレメンタリストリームを再構成し、デコードし、コンテンツをモニターに出力する。

【0066】

10

20

30

40

50

コンテンツ書き出し部 119 は、コンテンツを書き出すために必要な処理を行い、蓄積メディアに書き出す処理を行う。具体的には、コンテンツをメディアにバインドするために暗号変換したり、フォーマットを変換したり、といった処理を行う。

【0067】

図 5 は、書き出しコンテンツリスト蓄積部 114 に蓄積され、書き出しコンテンツリスト管理部 113 で管理される MCL のデータ構成の一例を示す図である。この MCL は、コンテンツ書き出し部 119 によって書き出されたコンテンツ及びコンテンツ表示部 118 により再生表示されたコンテンツを掲載したリストである。図示するように、この MCL は、コンテンツ ID に対応して書き出し回数、書き出し先、書き出し経路を含む。書き出し回数は、コンテンツ毎にコンテンツ書き出し部 119 によって蓄積メディアに何回書き出しを行ったかを示す。書き出し先は、DVD-RAM、D-VHS、SD カードなどの書き出しが許可される蓄積メディアを示す。書き出し経路は、アナログ出力、デジタル出力（圧縮／非圧縮）、出力画質（SD／HD）等の出力形態を示す。また、書き出しコンテンツリスト管理部 113 は、書き出し先、書き出し経路などの情報を、図 4 に示した ECM 内のプライベートデータから取得して MCL に設定してもよいし、放送波に含まれる情報（コンテンツ、ECM、PSI／SI 等）から取得して設定してもよいし、本コンテンツ利用システムが予め保持している値を設定してもよい。

【0068】

このように構成された MCL によれば、コンテンツ ID に対して、既にコンテンツを書き出した回数がわかるため、書き出しコンテンツリスト管理部 113 において、1 コンテンツ当たりの最大書き出し回数の範囲内に、コンテンツの書き出しを制限することが可能となる。

【0069】

以上のように構成されたコンテンツ利用システム 1 の動作を、図 6 および図 7 に示すフローチャートを用いて説明する。

図 6 は、コンテンツ取り込み装置 100 における、コンテンツ取り込み処理を示すフローチャートである。

【0070】

入力部 101 は、放送波からトランスポートストリームを受信する（ステップ S401）。

分離部 102 は、入力部 101 からトランスポートストリームを受け取り、TS パケットの PID を参照して、コンテンツの TS パケットや、ECM 等の TS パケットを分離する（ステップ S402）。コンテンツや ECM の TS パケットを示す PID は、PMT に記述されているので、これを参照して、TS パケットの分離を行う。

【0071】

コンテンツ鍵情報暗号変換部 103 は、ECM の TS パケットを受け取り、ECM セクションを再構成し、ワーク鍵を用いて暗号化された ECM を復号する（ステップ S403）。さらにコンテンツ鍵情報暗号変換部 103 は、復号された ECM 中のコピー制御情報がコピー禁止（COPY NEVER）である場合は、ネットワークにバインドしないので、以下の処理を行わない（コンテンツは再生表示可能）。NETWORK COPY である場合は、ネットワークにバインドするため以下を続行する。COPY FREE である場合は、必ずしもネットワークにバインドする必要はないが、書き出し回数を無制限としてネットワークにバインドしてもよい。

【0072】

コンテンツ鍵情報暗号変換部 103 は、コンテンツ ID 生成部 104 に対してコンテンツ ID 生成要求を送る。コンテンツ ID 生成部 104 はこれを受けて、コンテンツ ID を生成する（ステップ S404）。

【0073】

コンテンツ ID 生成部 104 は、生成したコンテンツ ID をコンテンツ鍵情報暗号変換部 103 に送る。コンテンツ鍵情報暗号変換部 103 は、取得したコンテンツ ID を ECM

10

20

30

40

50

に埋め込む（ステップS405）。具体的には、コンテンツID生成部104は、内部に保持するカウンタを用いてコンテンツIDを生成し、これをコンテンツ鍵情報暗号変換部103に送る。コンテンツ鍵情報暗号変換部103は、受け取ったコンテンツIDを、ECMの特定のフィールドに設定する。一例としては、図4に示すECMのプライベートデータ部に挿入する方法が挙げられる。

【0074】

コンテンツ鍵情報暗号変換部103は、ECMをネットワーク鍵で再暗号化する（ステップS406）。具体的には、コンテンツ鍵情報暗号変換部103は、ネットワークで予め共有された暗号鍵を内部で保持し、これを用いて、コンテンツIDを埋め込んだECMを再暗号化する。さらに、このように暗号化されたECMをTSパケット化して、多重化部105に渡す。

10

【0075】

多重化部105は、分離部102から受け取ったコンテンツのTSパケットと、コンテンツ鍵情報暗号変換部103から受け取った暗号変換後のECMのTSパケットとを多重化する（ステップS407）。

【0076】

多重化後のコンテンツとECMは記憶装置90に格納される。あるいは、記憶装置90に格納されると同時にコンテンツ利用装置110に入力される。

このように、コンテンツ取り込み装置100では、ECMの暗号が変換されることにより、ネットワークにバインドされたコンテンツが生成されると共に、コンテンツIDがECMに設定され、コンテンツと多重化される。

20

【0077】

一方、図7は、コンテンツ利用装置110における、コンテンツ書き出し処理を示すフローチャートである。

分離部111において、コンテンツ取り込み装置100から受け取ったトランスポートストリーム又は記憶装置90から読み出されたトランスポートストリームから、コンテンツとECMを分離する（ステップS501）。具体的には、トランスポートストリームのTSパケットのヘッダ部にあるPIDを参照し、それぞれのPIDに該当するTSパケットを分離する処理を行う。

【0078】

コンテンツ鍵情報復号部112は、分離部111からECMのTSパケットを受け取り、ECMセクションを再構成し、再暗号化されたECMを取得する。ECMの暗号化部分を予め取得してあるネットワーク鍵で復号する（ステップS502）。

30

【0079】

コンテンツ鍵情報復号部112は、復号したECMに埋め込まれているコンテンツIDを読み出す（ステップS503）。コンテンツ鍵情報復号部112は、該当コンテンツが書き出しを許可されているか否かを確認するため、読み出したコンテンツIDを書き出しコンテンツリスト管理部113に渡す。

【0080】

書き出しコンテンツリスト管理部113は、書き出しコンテンツリスト蓄積部114からMCLを読み出す（ステップS504）。書き出しコンテンツリスト管理部113は、まず、トランスポートストリームに含まれる情報（コンテンツ、ECM、PSI/SI等）から、または、システムが予め規定しているパラメータからコンテンツの書き出し先、書き出し経路の条件を取得し、ユーザが指定した書き出し先、書き出し経路が条件を満たすかどうかを確認する（ステップS505）。例えば、ユーザが書き出し先を「D-VHS」と指定し、コンテンツ利用装置110で予め備えられている書き出し先が「D-VHS」である場合は、該当コンテンツをD-VHSへ書き出すことができるが、コンテンツ利用装置110で予め備えられている書き出し先が「SDカード」であった場合は、書き出すことができない。書き出し経路についても同様に、ユーザの指定が、コンテンツ利用装置110で備えられている書き出し経路を満たさない限り、コンテンツを蓄積メディアに書

40

50

き出すことができない。

【0081】

さらに、書き出しコンテンツリスト管理部113は、コンテンツ鍵情報復号部112から受け取ったコンテンツIDがMCLに存在するか否かを判定する(ステップS506)。なお、書き出しコンテンツリスト蓄積部114にMCL自体が無かった場合(初期化されていない場合)は、MCLを生成する(初期化)する。

【0082】

ステップS506において、NOの場合、すなわちコンテンツIDがMCLに存在しない場合は、MCLを更新し、書き出しコンテンツリスト蓄積部114に蓄積する処理を行う(ステップS507)。この場合、該当コンテンツを書き出し可能であると判定している

10

【0083】

そして、該当コンテンツを書き出したことを記録するため、該当コンテンツID、書き出し回数、書き出し先、書き出し経路をMCLに追加し、MCLのハッシュを再計算して、MCLを書き出しコンテンツリスト蓄積部114に蓄積すると共に、書き出しコンテンツリスト管理部113で保持しているハッシュ値を、再計算したMCLのハッシュ値で置き換える。

【0084】

コンテンツ鍵情報復号部112は、ECMからコンテンツ鍵を取り出し、コンテンツ鍵をコンテンツ復号部116に渡すと共に、コンテンツ出力制御部115に対し、確認した書き出し先、書き出し経路で、当該コンテンツをコンテンツ書き出し部119へ渡すように指示を行う(ステップS508)。これにより、コンテンツ出力制御部115は、コンテンツ出力選択部117に対して、指定された書き出し先、書き出し経路でコンテンツを書き出すように制御する。

20

【0085】

コンテンツ復号部116は、分離部111から取得したTSパケットを、コンテンツ鍵情報復号部112から取得したコンテンツ鍵で復号(デスクランブル)する(ステップS509)。

【0086】

コンテンツ出力選択部117は、コンテンツ出力制御部115の制御に基づき、指定された書き出し先、書き出し経路で、コンテンツを書き出すためコンテンツ書き出し部119へコンテンツを渡す。

30

【0087】

コンテンツ書き出し部119は、コンテンツを蓄積メディアに書き出す(ステップS510)。具体的には、DVD-RAM、D-VHS等の蓄積メディアに対応した形式で、コンテンツを暗号化したり、フォーマット変換したりして、蓄積メディアにコンテンツを書き出す。

【0088】

ステップS506において、YESの場合、すなわちコンテンツIDがMCLに存在する場合は、MCLの該当コンテンツIDに関する情報を用いて、書き出し可否の確認を行う(ステップS511)。具体的には、MCLには、コンテンツID毎に書き出し回数、書き出し先、書き出し経路などが記録されるようになっており、これらを参照して、書き出し可能かどうかの確認を行う。

40

【0089】

例えば、コンテンツ毎に書き出し許容回数が「3」であり、書き出そうとするコンテンツのコンテンツIDが図5における「CONTENT-ID-11111」である場合、書き出し回数が「1」であるので、残り2回は書き出し可能であるため書き出し可能と判定される。このとき、書き出し先と書き出し経路については、MCLの内容が「-」、すなわち、書き出し先と書き出し経路については限定しないことを示しているため、ユーザの指定した書き出し先、書き出し経路での書き出しが可能である。また、コンテンツIDが

50

「CONTENT-ID-22222」、ユーザが指定した書き出し先が「DVD-RAM」である場合、書き出し回数が「2」、書き出し先が「DVD-RAM」であるので、書き出し可能と判定される。このとき、例えばユーザが指定した書き出し先が「SDカード」であった場合は、書き出し回数の制限を満たしている場合でも、書き出し先の制限を満たさないの、書き出し不可と判定される。また、コンテンツIDが、「CONTENT-ID-88888」、ユーザが指定した書き出し経路が「Dishell(SD)」である場合は、書き出し回数と書き出し経路の制限を共に満たすため、書き出し可能と判定されるが、ユーザが指定した書き出し経路が「Dishell(HD)」であった場合は、書き出し経路の制限を満たさないの、書き出し不可と判定される。さらに、「CONTENT-ID-77777」である場合は、既に書き出し回数が「3」であるので、書き出し不可と判定される。

10

【0090】

ステップS511において、YESの場合、すなわち書き出し可能と判定された場合は、MCLを更新、蓄積する(ステップS507)。ステップS507以降の処理の詳細については前述の通りであるので、以降は省略する。

【0091】

ステップS511において、NOの場合、すなわち書き出し不可と判定された場合は、コンテンツ書き出し処理を終了する。

このように、本コンテンツ利用システム1では、ネットワークバインドされたコンテンツにコンテンツIDを付与し、コンテンツを書き出す際に、MCLで書き出し確認を行うことにより、無制限なコンテンツの書き出しに制限を課するようになっている。

20

【0092】

また、図7では、コンテンツ利用装置110における、コンテンツ書き出し処理のフローチャートを示したが、図8では、コンテンツ再生(表示)処理を示すフローチャートが示されている。

【0093】

図8において、ステップS601~S606の処理については、図7に示したコンテンツ書き出し処理と同様であるので、ここでは省略する。

ステップS606において、NOの場合、すなわちMCLに該当コンテンツIDが存在しない場合は、該当のコンテンツを書き出していないので、再生処理可能と判定し、コンテンツ鍵情報復号部112は、ECMからコンテンツ鍵を取り出し、コンテンツ復号部116に渡す処理を行う(ステップS608)。

30

【0094】

コンテンツ復号部116は、分離部111から取得したTSパケットを、コンテンツ鍵情報復号部112から取得したコンテンツ鍵で復号(デスクランブル)する(ステップS609)。

【0095】

コンテンツ出力選択部117は、コンテンツ出力制御部115の制御に基づき、コンテンツを表示するためのコンテンツ表示部118へコンテンツを渡す。

コンテンツ表示部118は、コンテンツをTV等に出力する(ステップS610)。

40

【0096】

ステップS606において、YESの場合、すなわちMCLに該当コンテンツIDが存在する場合は、MCLの該当コンテンツIDに関する情報を用いて再生可否の確認を行う(ステップS607)。具体的には、書き出し回数が書き出し上限回数に達しているか否かを確認し、書き出し上限回数に達していない場合は再生可、書き出し上限回数に達している場合は再生不可と判定する。

【0097】

ステップS607において、YESの場合、すなわち再生可の場合は、ステップS608以降を実行する。

ステップS607において、NOの場合、すなわち再生不可の場合は、コンテンツ再生処

50

理を終了する。

【0098】

このように、本コンテンツ利用システム1では、蓄積メディアに書き出したコンテンツであっても、ネットワーク内にコンテンツのコピーが存在する可能性があるため、書き出したコンテンツの表示（再生）処理時においても、MCSを用いてコンテンツの再生が可能か否かを確認することで、利用に制限を課するようにしている。

【0099】

ところで、電源断やユーザキャンセル等により、書き出し処理が中断（失敗）してしまう場合が発生する。そのため、本コンテンツ利用システム1では、このような場合において、書き出し処理を再開することができるようになっている。具体的には、図3において、コンテンツ鍵情報復号部112において、スクランブル単位（例えば、ECMに含まれるコンテンツ鍵が更新される単位）にID（以降、スクランブルIDと記す）を付与し、コンテンツ復号部116はコンテンツ鍵と前記スクランブルIDを受け取り、どこまでコンテンツ書き出し部119にコンテンツを渡したか、すなわち、どこまで蓄積メディアへの書き出しが成功したかを保持しておく。キャンセルが発生し、書き出し処理を再開する場合には、コンテンツ復号部116は、保持しているスクランブルIDをコンテンツ鍵情報復号部112に送信することにより、該当するスクランブルIDから処理を再開することができるようになっている。

【0100】

この処理について、図9および図10に示すフローチャートを用いて説明する。

図9は、コンテンツの蓄積メディアへの書き出し処理を示すフローチャートである。同図では、書き出しを開始し、中断（キャンセルやポーズ）するまで、及び終了するまでの処理を示している。

【0101】

コンテンツの書き出し処理が開始されると、書き出しコンテンツリスト管理部113は、書き出すコンテンツのコンテンツIDを仮登録する（ステップS701）。

【0102】

コンテンツ鍵情報復号部112は、書き出し処理中断（キャンセル）原因が発生しているかどうかをチェックする（ステップS702）。処理中断でない場合はステップS703を実行し、処理中断の場合は、コンテンツ書き出し処理を終了する。電源断の場合も当然に終了する。

【0103】

ステップS703では、コンテンツを全スクランブル単位分出力したか否かを判定する。全スクランブル単位を出力していない場合は、ステップS704を実行し、全スクランブル単位を出力した場合は、ステップS709を実行する。

【0104】

コンテンツ鍵情報復号部112は、スクランブル単位毎にスクランブルIDを付与する（ステップS704）。具体的には、スクランブル単位毎に単調増加するIDを付与することにより、コンテンツ復号部116あるいはコンテンツ書き出し部119が、どこまで書き出したかを識別するIDとして用いることができる。また、最後に付与したスクランブルIDを、最終送出スクランブルIDとして、内部に保持する。

【0105】

コンテンツ鍵情報復号部112は、ECMからコンテンツ鍵を読み出し、コンテンツ復号部116に、コンテンツ鍵とスクランブルIDとを渡す（ステップS705）。ここで、複数のコンテンツの書き出し処理が中断される場合を考慮し、スクランブルIDと共に、書き出すコンテンツのコンテンツIDを渡すようにしてもよい。

【0106】

コンテンツ復号部116は、コンテンツ鍵とスクランブルIDを受信する（ステップS706）。

コンテンツ復号部116は、暗号化されたコンテンツをコンテンツ鍵で復号し、書き出し

10

20

30

40

50

が完了したスクランブル単位のスクランブルIDを内部に保持する（ステップS707）。

【0107】

コンテンツ書き出し部119は、コンテンツを書き出す（ステップS708）。
ステップS703でコンテンツを全スクランブル単位分出力したと判定した場合は、書き出しコンテンツリスト管理部113は、書き出すコンテンツのコンテンツIDをMCLへ本登録する（ステップS709）。

【0108】

なお、ここではコンテンツ復号部116で暗号化されたコンテンツを復号した時点で、スクランブルIDを内部に保持するようにしたが、コンテンツ書き出し部119からコンテンツを書き出し、蓄積メディアに正常に書き込まれた旨の通知を受けてから、スクランブルIDを内部に保持するようにしても良い。

10

【0109】

図10は、処理の中断が発生後、処理を再開（継続）する処理を示している。同図の処理は、MCLに仮登録されたコンテンツIDが発見された場合や、ユーザにより再開要求を受けた場合等に開始する。

【0110】

同図において、コンテンツ復号部116は、コンテンツ鍵情報復号部112に、保持しているスクランブルIDを送信する（ステップS801）。

コンテンツ鍵情報復号部112は、スクランブルIDを受信する（ステップS802）。

20

【0111】

コンテンツ鍵情報復号部112は、保持している最終送出スクランブルIDと、コンテンツ復号部116から受け取ったスクランブルIDを比較する（ステップS803）。具体的には、コンテンツ復号部116から受け取ったスクランブルIDと、最終送出スクランブルIDの差分を求め、差分が予め設定された値以下であるか否かを判定すること、不正な書き出しを防止する。

【0112】

ステップS803において、YESの場合、すなわち差分が値以下の場合は、書き出し処理の再開を許可し、コンテンツ書き出し処理を再開する（ステップS804）。なお、コンテンツ書き出し処理の再開後の動作については、図9で説明しているため、ここでは省略する。

30

【0113】

ステップS803において、NOの場合、すなわち差分が値より大きい場合は、コンテンツ書き出し処理を中止する（ステップS805）。

このように、本コンテンツ利用システム1では、コンテンツの書き出しに際して、書き出しの進捗を識別するためのスクランブルIDを付与するようにしているため、コンテンツ書き出し時の電源断、ユーザによる中断などがあった場合でも、セキュリティ上、安全に再開することができるようになっている。

【0114】

（実施の形態2）

40

以下、本発明の実施の形態2について、図面を用いて詳細に説明する。

図11は、本発明の実施の形態2に係るコンテンツ利用システム2の構成を示すブロック図である。なお、本図において、図3に示した実施の形態1のコンテンツ利用システム1と同様の構成要素については、図3において既に説明しているため、図3と同様の符号を付して以下の説明を省略する。

【0115】

図11に示すコンテンツ利用システム2では、コンテンツ取り込み装置100は本発明の実施の形態1に挙げたコンテンツ利用システム1と同様の構成であるが、コンテンツ利用装置110αが、さらに書き出しコンテンツリスト同期部901を備えており、ネットワーク接続された他のコンテンツ利用装置110αと通信を行い、複数のコンテンツ利用装

50

置 110α間ではMCLの同期を行うことを特徴とする。

【0116】

書き出しコンテンツリスト同期部901は、他のコンテンツ利用装置110αとの間でMCLの同期情報を送受信することによってMCLの同期を取り、その結果を書き出しコンテンツリスト管理部113に通知する。具体的には、コンテンツの書き出しを行い、MCLを更新したタイミングで、書き出しコンテンツリスト管理部113は、書き出しコンテンツリスト同期部901に対し、更新したコンテンツIDに関する同期情報を渡す。書き出しコンテンツリスト同期部901は、この同期情報をネットワーク接続された他のコンテンツ利用装置110αに送信する。この同期情報を受信した他のコンテンツ利用装置110αの書き出しコンテンツリスト同期部901は、同期情報を書き出しコンテンツリスト管理部113に渡し、この情報を書き出しコンテンツリスト蓄積部114のMCLに反映することにより、MCLの同期を確保する。同期する情報（同期情報）の一例としては、書き出したコンテンツIDを含む、MCLに記録された情報である。また、同期方法の一例としては、ネットワーク上に同期情報をブロードキャストする方法が挙げられる。

【0117】

図12は、書き出しコンテンツリスト同期部901が、ネットワーク接続された他のコンテンツ利用装置110αの書き出しコンテンツリスト同期部901とMCLの同期をとる場合のシーケンス図である。本図では、MCLの更新元（MCLを更新し、同期情報をブロードキャストするコンテンツ利用装置110α）を第1のコンテンツ利用装置110α、MCLの更新先（ブロードキャストされた同期情報を受信し、MCLを更新するコンテンツ利用装置110α）を第2のコンテンツ利用装置110βとする。なお、MCLの更新先に相当するコンテンツ利用装置110αは、複数存在する可能性があるが、第2のコンテンツ利用装置110βをその代表として示している。

【0118】

第1のコンテンツ利用装置110αの書き出しコンテンツリスト管理部113は、コンテンツを書き出す場合、コンテンツ鍵情報復号部112から該当コンテンツのコンテンツIDを取得し、書き出しコンテンツリスト蓄積部114から読み出したMCLを更新する（ステップS1001）。具体的には、コンテンツIDが「CONTENT-ID-12345」であるコンテンツを書き出した場合、図13に示すように、第1のコンテンツ利用装置110αが保持するMCLには、「CONTENT-ID-12345」のコンテンツIDに関する情報（コンテンツID、書き出し回数など）が追加されている。このとき、図14に示したように、第2のコンテンツ利用装置110βが保持するMCLには、第1のコンテンツ利用装置110αが「CONTENT-ID-12345」なるコンテンツIDのコンテンツを書き出したことは通知されていないため、「CONTENT-ID-12345」のレコードは存在しない。

【0119】

なお、図13に示すMCLでは、コンテンツの書き出し回数を示す情報に関して、書き出しを行った回数（書き出し回数）と、書き出し可能な最大回数（最大書き出し回数）が記録されるようになっている。よって、コンテンツの再生を制御する場合に、書き出し回数が最大書き出し回数に達していない間は、該当コンテンツの再生が可能であるが、最大書き出し回数に達した場合は、該当コンテンツの再生を不可とする制御を行う。また、ここでは書き出し回数として、既に書き出した回数を記録するようにしたが、書き出し可能な残り回数を記録するようにし、書き出しを行う都度、書き出し回数を減算していくようにしても良い。この場合は、書き出し回数が0となった時点で、該当コンテンツの書き出し及び再生が不可となる。

【0120】

第1のコンテンツ利用装置110αの書き出しコンテンツリスト管理部113は、更新したコンテンツIDに関する情報を、書き出しコンテンツリスト同期部901に通知する（ステップS1002）。具体的には、第1のコンテンツ利用装置110αの書き出しコンテンツリスト管理部113は、図13に示す第1のコンテンツ利用装置110αのMCL

10

20

30

40

50

において、コンテンツIDが「CONTENT-ID-12345」のレコード全てを書き出しコンテンツリスト同期部901に通知する。

【0121】

第1のコンテンツ利用装置110αの書き出しコンテンツリスト同期部901は、書き出しコンテンツリスト管理部113から受け取った、コンテンツIDが「CONTENT-ID-12345」に関する情報から、同期情報を生成する（ステップS1003）。同期情報の一例としては、図15に示すような同期情報1301が挙げられる。同期情報1301は以下の情報から構成されている。

【0122】

セッションID（SESSION-ID）は、コンテンツ利用装置110α毎に同期情報を生成する度に設定される。具体的には、カウンタなどで実現され、同期情報を生成する度に1を加算されるIDである。

【0123】

コンテンツ利用装置ID（TERMINAL-ID）は、コンテンツ利用装置110αが内部に保持し、コンテンツ利用装置110αを識別するためのIDであり、例えば、複数のコンテンツ利用装置110αにおいて、同時に同一コンテンツIDのコンテンツを書き出し、双方の同期情報がブロードキャストされた場合などに、両者を正確に区別するための情報として用いられる。

【0124】

コンテンツID（CONTENT-ID）は、書き出したコンテンツのコンテンツIDである。

書き出し回数、書き出し先、書き出し経路は、基本的にMCLの情報と同一である。なお、同期情報としてMCLそのものを用いても良いが、以下の説明では、同期情報として、図15に示す同期情報1301を用いる。

【0125】

次に、第1のコンテンツ利用装置110αの書き出しコンテンツリスト同期部901は、生成した同期情報1301を送信する（ステップS1004）。具体的には、第1のコンテンツ利用装置110αの書き出しコンテンツリスト同期部901は、同期情報1301をネットワークにブロードキャストする。

【0126】

第2のコンテンツ利用装置110βの書き出しコンテンツリスト同期部901は、ブロードキャストされた同期情報1301を受信し、書き出しコンテンツリスト管理部113に対し、MCLを読み出すよう要求を行う。（ステップS1005）。

【0127】

書き出しコンテンツリスト蓄積部114からMCLを読み出し、第2のコンテンツ利用装置110βの書き出しコンテンツリスト管理部113は、MCLのハッシュを計算し、書き出しコンテンツリスト管理部113が保持しているハッシュ値と比較して、その正当性を確認し、その内容を書き出しコンテンツリスト同期部901に渡す（ステップS1006）。なお、MCLが書き出しコンテンツリスト蓄積部114に存在しない場合は、MCLを生成（初期化）する。

【0128】

第2のコンテンツ利用装置110βの書き出しコンテンツリスト同期部901は、セッションIDやコンテンツ利用装置ID等を確認し、書き出しコンテンツリスト管理部113から受け取ったMCLの内容と、同期情報1301とを比較し、同期情報1301をMCLに反映するかどうかの判定を行う（ステップS1007）。具体的には、同期情報1301の内容が、MCLの内容に含まれていないか、あるいは、更新されていないかを判定することによって行われる。

【0129】

ステップS1007において、YESの場合、すなわちMCLを更新する必要があると判定された場合には、書き出しコンテンツリスト同期部901は、書き出しコンテンツリス

10

20

30

40

50

ト管理部 113 に同期情報 1301 の内容を通知し、書き出しコンテンツリスト管理部 113 は、MCL を同期情報 1301 の内容で更新する（ステップ S1008）。具体的には、図 14 に示した第 2 のコンテンツ利用装置 110β の保持する MCL の内容が、図 13 に示した第 1 のコンテンツ利用装置 110α が保持する MCL の内容に一致するよう同期される。

【0130】

第 2 のコンテンツ利用装置 110β の書き出しコンテンツリスト管理部 113 は、MCL のハッシュを再計算し、ハッシュ値を内部で保持し、MCL を書き出しコンテンツリスト蓄積部 114 に書き込む（ステップ S1009）。

【0131】

ステップ S1007 において、NO の場合、すなわち MCL を更新する必要がないと判定された場合には、本同期処理を終了する。具体的には、同期情報 1301 は複数回繰り返してブロードキャストされる可能性があるため、同期情報 1301 のセッション ID と同期情報送信元のコンテンツ利用装置 ID を参照して、複数回同じ同期情報 1301 を受信した場合には、不要な同期情報 1301 を破棄する処理を行う。

【0132】

なお、コンテンツ取り込み装置 100 におけるコンテンツ取り込み処理、および、コンテンツ利用装置 110α におけるコンテンツ書き出し処理、および、コンテンツ利用装置 110α におけるコンテンツ再生処理については、本発明の実施の形態 1 と同様であり、既に説明しているため、ここでは説明を省略する。

【0133】

このように、本コンテンツ利用システム 2 では、ネットワーク上の複数のコンテンツ利用装置 110α 間で MCL を同期するようにしている。そのため、本発明の実施の形態 1 で示したコンテンツ利用システム 1 が、書き出し可能なコンテンツ数などの制限をコンテンツ利用装置 110α 毎に課していたのに対し、ネットワーク全体、すなわち複数のコンテンツ利用装置 110α 全体に対して課するようにすることができる。

【0134】

（実施の形態 3）

以下、本発明の実施の形態 3 について、図面を用いて詳細に説明する。

図 16 は、本発明の実施の形態 3 に係るコンテンツ利用システム 3 の構成を示すブロック図である。なお、本図において、図 3 に示した実施の形態 1 のコンテンツ利用システム 1 と同様の構成要素については、図 3 において既に説明しているため、図 3 と同様の符号を付して以下の説明を省略する。

【0135】

図 16 に示すコンテンツ利用システム 3 は、本発明の実施の形態 1 に挙げたコンテンツ利用システム 1 に対して、コンテンツ取り込み装置 100 が、さらに書き出しコンテンツリスト管理部 1401 と、書き出しコンテンツリスト蓄積部 1402 と、コンテンツ ID 受信部 1403 とを備え、コンテンツ利用装置 110β が、分離部 111 と、コンテンツ鍵情報復号部 112 と、コンテンツ出力制御部 115 と、コンテンツ復号部 116 と、コンテンツ出力選択部 117 と、コンテンツ出力部としてコンテンツ表示部 118 およびコンテンツ書き出し部 119 と、コンテンツ ID 送信部 1404 とを備えており、コンテンツ取り込み装置 100 が MCL を管理し、コンテンツ利用装置 110β は、コンテンツを書き出したり、表示（再生）したりする場合において、コンテンツ取り込み装置 100 に書き出し可否を問い合わせ、コンテンツ取り込み装置 100 での書き出し可否判定の結果に基づいて、コンテンツの書き出しおよび表示を制御することとを特徴とする。

【0136】

また、コンテンツ利用システム 3 で管理する MCL は、コンテンツ利用システム 3 に取り込んだコンテンツに付与したコンテンツ ID を MCL に全て登録し、MCL の内、書き出したコンテンツのコンテンツ ID のみにマーキングをするようにしている。そのため、コンテンツ ID 生成部 104 は、新たにコンテンツを取り込む場合にコンテンツ ID を生成

10

20

30

40

50

し、書き出しコンテンツリスト管理部 1401 にコンテンツ ID を通知する必要がある。

【0137】

コンテンツ取り込み装置 100 における書き出しコンテンツリスト管理部 1401 は、書き出しコンテンツリスト蓄積部 1402 に蓄積している MCL を読み出し、MCL の参照、更新処理等を行う。具体的には、MCL に登録するコンテンツ ID をコンテンツ ID 生成部 104 から受け取り、MCL にコンテンツ ID を登録したり、書き出すコンテンツのコンテンツ ID をコンテンツ利用装置 110b から受けた場合に、書き出し可否を判定し、MCL を更新する、といった処理を行う。また、MCL が書き出しコンテンツリスト蓄積部 1402 に蓄積されていない場合は、MCL を新たに生成し、初期化する。なお、MCL のハッシュを計算し、セキユアに管理する方法については、本発明の実施の形態 1 において説明しているため、ここでは記述を省略する。

10

【0138】

コンテンツ取り込み装置 100 における書き出しコンテンツリスト蓄積部 1402 は、MCL を蓄積しておく部であり、ハードディスク等によって実現される。

【0139】

コンテンツ取り込み装置 100 におけるコンテンツ ID 受信部 1403 は、コンテンツ利用装置 110b のコンテンツ ID 送信部 1404 から、書き出しあるいは再生するコンテンツのコンテンツ ID を受信し、コンテンツ ID を書き出しコンテンツリスト管理部 1401 に渡し、書き出しコンテンツリスト管理部 1401 から受け取った書き出し可否判定結果をコンテンツ利用装置 110b のコンテンツ ID 送信部 1404 に送信する処理を行う。

20

【0140】

コンテンツ利用装置 110b におけるコンテンツ ID 送信部 1404 は、コンテンツ鍵情報復号部 112 から書き出しまたは再生を行うコンテンツのコンテンツ ID を受信し、コンテンツ ID をコンテンツ取り込み装置 100 のコンテンツ ID 受信部 1403 に送信し、コンテンツ取り込み装置 100 での書き出し可否判定の結果を受信し、コンテンツ鍵情報復号部 112 に渡すといった処理を行う。

【0141】

また、本発明の実施の形態 1 におけるコンテンツ利用システム 1、および、本発明の実施の形態 2 におけるコンテンツ利用システム 2 では、コンテンツ ID を ECM に設定する例を示したが、ここでは ECM (コンテンツ鍵情報) 以外の情報に設定する場合を示す。ECM 以外の情報の一例として、コンテンツ ID を PMT に設定したり、Private セクションとしてコンテンツ ID を設定し、PMT から PID でポイントングする等の方法が挙げられる。PMT にコンテンツ ID を設定する一例として、図 17 では、PMT の `descriptor` 部の第 1 ループ部に、コンテンツ ID を設定できるように規定された `content-id-descriptor` を挿入する場合を示している。PMT の `descriptor` 部には、システム毎に規定される任意のディスクリプタが設定できるようにしており、デジタルコピーに関する情報を記したデジタルコピー制御記述子や、CAS の限定受信方式記述子などが挿入されたりする。本コンテンツ利用システムでは、この `descriptor` 部に、新たに `content-id-descriptor` を規定し、この中の `content-id` フィールドにコンテンツ ID を設定するようにしている。ちなみに、ディスクリプタを第 1 ループ部に設定するか、第 2 ループ部に設定するかは、システムによって任意であるが、プログラム毎のパラメータの場合は第 1 ループ部に、エレメンタリ毎のパラメータの場合は第 2 ループ部に設定されるのが一般的である。以下の説明では、PMT にコンテンツ ID を挿入する例を示す。

30

40

【0142】

ところで、上述のように、コンテンツ ID を ECM 以外に挿入する場合、コンテンツ ID の不正な付け替えや改ざん等が行われてしまう危険性があるため、コンテンツとコンテンツ ID とをセキユアにバインドする必要がある。そこで、コンテンツ取り込み装置 100 におけるコンテンツ鍵情報暗号変換部 103 は、ECM を暗号変換する際に、コンテンツ

50

IDを関連付けて暗号変換を行うことで、コンテンツとコンテンツIDとをセキュアにバインドする。具体的には、ネットワーク鍵とコンテンツIDのXOR (Exclusive OR)をとったものや、ネットワーク鍵とコンテンツIDを結合したものを、ECMを再暗号化する暗号鍵として用いる方法や、コンテンツIDのハッシュをSHA-1等のハッシュアルゴリズムを用いて計算し、このハッシュ値をECMに挿入する方法や、ECMをコンテンツIDで暗号化した後、さらにネットワーク鍵で暗号化する方法などが挙げられる。以下の説明では、ネットワーク鍵とコンテンツIDのXORをとったものを、ECMを再暗号化する暗号鍵として用いる例を示す。

【0143】

以上のように構成されたコンテンツ利用システム3の動作を、図18および図20に示すフローチャートを用いて説明する。 10

図18は、コンテンツ取り込み装置100における、コンテンツ取り込み処理を示すフローチャートである。

【0144】

入力部101は、放送波からトランスポートストリームを受信する(ステップS1501)。

分離部102は、入力部101からトランスポートストリームを受け取り、TSパケットのPIDを参照して、コンテンツのTSパケットとECMのTSパケットを分離する(ステップS1502)。コンテンツおよびECMのTSパケットを示すPIDは、PMTに記述されているので、これを参照して、TSパケットの分離を行う。また、コンテンツIDを生成するため、SI情報を分離する。例えば、イベント情報が記述されたEIT(Event Information Table)や現在時刻が記述されたTOT(Time Offset Table)などである。 20

【0145】

コンテンツ鍵情報暗号変換部103は、ECMのTSパケットを受け取り、ECMセクションを再構成し、ワーク鍵を用いて暗号化されたECMを復号する(ステップS1503)。

【0146】

コンテンツ鍵情報暗号変換部103は、コンテンツID生成部104に対してコンテンツと共に配信されるデータ(EIT、TOTの情報等)と共にコンテンツID生成要求を送り、コンテンツID生成部104はこれを受けて、コンテンツIDを生成する(ステップS1504)。ここで、コンテンツID生成部104は、例えばEITのservice-idと、TOTの現在時刻からコンテンツIDを生成する。この場合、コンテンツIDは時間単位で与えられることになる。さらに、このときにコンテンツ取り込み装置100が内部で保持するユニークなIDを関連づけてコンテンツIDを生成すれば、グローバルユニークなコンテンツIDとすることができ、このように生成したコンテンツIDを、MCLを更新するために書き出しコンテンツリスト管理部1401に渡すと共に、コンテンツIDを記述したcontent-id-descriptionを生成するために多重化部105に渡す。また、コンテンツとコンテンツIDをセキュアにバインドするため、コンテンツIDをコンテンツ鍵情報暗号変換部103に渡す。 30

【0147】

書き出しコンテンツリスト管理部1401は、コンテンツID生成部104からコンテンツIDなどを受けると、書き出しコンテンツリスト蓄積部1402からMCLを読み出し(ステップS1505)、コンテンツID生成部104から受け取ったコンテンツIDを登録する(ステップS1506)。なお、書き出しコンテンツリスト蓄積部1402にMCLが無い場合は、MCLを生成して初期化を行う。 40

【0148】

ここで、MCLは図19に示すように構成される。図19に示したMCLでは、現在までに蓄積メディアにコンテンツを書き出した回数として書き出し回数を記録すると共に、ある単位時間あたりの書き出し回数の上限(上限回数/単位)、および、あるコンテンツを 50

書き出してから、一定時間は当該コンテンツを書き出し不可とする制御を行うためのインターバルの時間（ペナルティ時間）、および、前回書き出しを行った時刻（前回書き出し時刻）とを記録するようになっている。例えば、コンテンツIDが「CONTENT-ID-11111」のコンテンツは、書き出しが1回行われていることを示しているが、単位時間あたりの書き出し回数の上限は、「2/DaY」であるので、1日の間に2回は書き出すことができ、あと1回は蓄積メディアに書き出すことができることになる。また、ペナルティ時間については、「1hour」となっているため、前回書き出し時刻である「22:22:22」から1時間の間（即ち、23:22:22まで）は当該コンテンツを蓄積メディアに書き出すことが不可となるようなペナルティが課されるよう制御される。なお、本実施の形態では、単位時間あたりの書き出し回数の上限や、ペナルティ時間の設定を、コンテンツ毎に行うようにしたが、これらのパラメータをMCL毎に設定するようにし、MCL毎に全コンテンツ共通の制約として用いても良い。

10

【0149】

また、書き出したコンテンツにマーキングを行う処理として、本実施の形態では、書き出し回数をインクリメントする（書き出していないコンテンツの場合は0のままである）ことにより、書き出したコンテンツと、一度も書き出していないコンテンツを区別するようにしている。

【0150】

書き出しコンテンツリスト管理部1401は、更新したMCLを書き出しコンテンツリスト蓄積部1402に書き込む（ステップS1507）。

20

コンテンツ鍵情報暗号変換部103は、コンテンツID生成部104から受け取ったコンテンツIDとネットワーク鍵とを用いて、復号されたECMを再暗号化する（ステップS1508）。具体的には、コンテンツ鍵情報暗号変換部103は、内部で保持しているネットワークで予め共有された暗号鍵とコンテンツIDとのXORをとり、これを用いてECMを再暗号化する。さらに、このように再暗号化されたECMをTSパケット化して、多重化部105に渡す。

【0151】

多重化部105は、分離部102から受け取ったコンテンツのTSパケットと、コンテンツ鍵情報暗号変換部103から受け取った暗号変換後のECMのTSパケットとを多重化する。また、コンテンツID生成部104から受け取ったコンテンツIDからcontent-id-descriptorを生成し、PMTのディスクリプタ部に挿入する（ステップS1509）。

30

【0152】

このように、コンテンツ取り込み装置100では、ECMの暗号が変換されることにより、ネットワークにバインドされたコンテンツが生成されると共に、コンテンツIDがPMTに設定され、コンテンツと多重化される。また、MCLに取り込んだコンテンツのコンテンツIDが登録される。

【0153】

一方、図20は、コンテンツ利用装置110bにおける、コンテンツ書き出し処理を示すフローチャートである。但し、コンテンツの書き出し可否をコンテンツ取り込み装置100に問い合わせる処理を行うため、コンテンツ取り込み装置100での処理も併せて図示している。

40

【0154】

分離部111において、コンテンツ取り込み装置100から受け取ったトランスポートストリームから、コンテンツとECMを分離する。また、PMTを分離し、PMTのディスクリプタ部のcontent-id-descriptorからコンテンツIDを取得し、コンテンツ鍵情報復号部112に通知する（ステップS1701）。

【0155】

コンテンツ鍵情報復号部112は、分離部111から取得したコンテンツIDを、コンテンツID送信部1404に渡し、コンテンツID送信部1404は、コンテンツIDをコ

50

ンテンツ取り込み装置 100 に送信する (ステップ S 1702)。

【0156】

コンテンツ取り込み装置 100 のコンテンツ ID 受信部 1403 は、コンテンツ ID を受信し (ステップ S 1703)、受信したコンテンツ ID を書き出しコンテンツリスト管理部 1401 に渡す。

【0157】

書き出しコンテンツリスト管理部 1401 は、書き出しコンテンツリスト蓄積部 1402 から MCL を読み出す (ステップ S 1704)。

書き出しコンテンツリスト管理部 1401 は、コンテンツ ID と MCL とから、該当コンテンツの外部書き出し可否判定を行う (ステップ S 1705)。具体的には、MCL に登録されているコンテンツ ID の単位時間あたりの上限回数や、ペナルティ時間を参照し、書き出しについて、制限内か否かを判定する処理を行う。

【0158】

ステップ S 1705 において、YES の場合、すなわち判定結果が書き出し可の場合、MCL の書き出し回数に 1 を加算して MCL を更新し、書き出しコンテンツリスト蓄積部 1402 に蓄積する (ステップ S 1706)。また、判定結果をコンテンツ ID 受信部 1403 に送信する。

【0159】

ステップ S 1705 において、NO の場合、すなわち判定結果が書き出し不可の場合、判定結果をコンテンツ ID 受信部 1403 に送信する。

コンテンツ取り込み装置 100 のコンテンツ ID 受信部 1403 は、書き出しコンテンツリスト管理部 1401 から受け取った書き出し可否の判定結果を、コンテンツ利用装置 110b に送信する (ステップ S 1707)。

【0160】

コンテンツ利用装置 110b のコンテンツ ID 送信部 1404 は、コンテンツ利用装置 110b から書き出し可否の判定結果を受信し、判定結果をコンテンツ鍵情報復号部 112 に渡す (ステップ S 1708)。

【0161】

コンテンツ鍵情報復号部 112 は、書き出し可否の判定結果に従い、コンテンツの書き出し処理を行うかどうかを決定する (ステップ S 1709)。

ステップ S 1709 において、YES の場合、すなわち判定結果が書き出し可である場合、コンテンツ鍵情報復号部 112 は、分離部 111 から取得した再暗号化された ECM を取得し、ネットワーク鍵とコンテンツ ID との XOR をとり、これを用いて ECM を復号する (ステップ S 1710)。

【0162】

コンテンツ鍵情報復号部 112 は、ECM からコンテンツ鍵を取り出し、コンテンツ鍵をコンテンツ復号部 116 に渡すと共に、コンテンツ出力制御部 115 に対し、当該コンテンツをコンテンツ書き出し部 119 へ渡すように指示を行う (ステップ S 1711)。これにより、コンテンツ出力制御部 115 は、コンテンツ出力選択部 117 に対してコンテンツを書き出すように制御する。

【0163】

コンテンツ復号部 116 は、分離部 111 から取得した TS パケットを、コンテンツ鍵情報復号部 112 から取得したコンテンツ鍵で復号 (デスクランブル) する (ステップ S 1712)。

【0164】

コンテンツ出力選択部 117 は、コンテンツ出力制御部 115 の制御に基づき、コンテンツを書き出すためのコンテンツ書き出し部 119 へコンテンツを受け渡す (ステップ S 1713)。

【0165】

コンテンツ書き出し部 119 は、コンテンツを蓄積メディアに書き出す (ステップ S 1714)。

10

20

30

40

50

14)。具体的には、DVD-RAM、D-VHS等の蓄積メディアに対応した形式で、コンテンツを暗号化したり、フォーマット変換したりして、蓄積メディアにコンテンツを書き出す。

【0166】

ステップS1709において、NOの場合、すなわち判定結果が書き出し不可である場合、コンテンツ鍵情報復号部112は、コンテンツ書き出し処理を中止する。

【0167】

このように、本コンテンツ利用システム3では、ネットワークバインドされたコンテンツにコンテンツIDを付与し、同時にコンテンツ取り込み装置100において管理するMC LにコンテンツIDを登録し、コンテンツ利用装置110bは、コンテンツを書き出す際に、コンテンツ取り込み装置100に書き出し可否を問い合わせ、コンテンツ取り込み装置100がMC Lを用いて書き出し可否を判定することにより、無制限なコンテンツの書き出しに制限を課するようになっている。

【0168】

また、コンテンツ利用装置110bにおける、コンテンツ再生（表示）処理については、図20と同様の処理の流れであるため、ここでは省略する。但し、ステップS1706の処理は常に行われないうこと、および、コンテンツ出力制御部115からの指示により、ステップS1712でコンテンツ出力選択部117がコンテンツをコンテンツ表示部118に渡す処理を行い、コンテンツを再生する、というように修正が必要である。

【0169】

（実施の形態4）

以下、本発明の実施の形態4について、図面を用いて詳細に説明する。

図21は、本発明の実施の形態4に係るコンテンツ利用システム4の構成を示すブロック図である。なお、本図において、図16に示した実施の形態3のコンテンツ利用システム3と同様の構成要素については、図16において既に説明しているもので、図16と同様の符号を付して以下の説明を省略する。

【0170】

図21に示すコンテンツ利用システム4は、本発明の実施の形態3に挙げたコンテンツ利用システム3に対して、コンテンツ取り込み装置100が、コンテンツID受信部1403に代えて、書き出しコンテンツリスト送信部1801を備え、コンテンツ利用装置110cが、コンテンツID送信部1404に代えて、書き出しコンテンツリスト受信部1802を備え、さらに、書き出しコンテンツリスト管理部1803と、書き出しコンテンツリスト蓄積部1804とを備え、コンテンツ取り込み装置100がMC Lを管理し、コンテンツ利用装置110cは、コンテンツ取り込み装置100からMC Lのコピーを受信し、受信したMC Lに基づいて、コンテンツの書き出しおよび表示を制御することとを特徴とする。

【0171】

コンテンツ取り込み装置100における書き出しコンテンツリスト送信部1801は、書き出しコンテンツリスト蓄積部1402に蓄積されているMC Lが更新されたとき、コンテンツ利用装置110cにMC Lを送信する。具体的には、コンテンツ取り込み装置100が新たにコンテンツを取り込むことにより、MC LにコンテンツIDを登録する、あるいは、コンテンツ利用装置110cにおいて、コンテンツを書き出すことにより、コンテンツ利用装置110cから書き出したコンテンツのコンテンツIDを受信し、MC Lの該当コンテンツIDに書き出した旨を表すマーキングを行ったときに、MC Lを各コンテンツ利用装置110cに送信する。送信方法の一例としては、ブロードキャストする方法が挙げられる。

【0172】

コンテンツ利用装置110cにおける書き出しコンテンツリスト受信部1802は、コンテンツを書き出したとき、書き出したコンテンツのコンテンツIDをコンテンツ取り込み装置100に送信し、コンテンツ取り込み装置100において、MC Lが更新されたとき

10

20

30

40

50

に、バージョンが更新された新しいMCLを受信する処理を行う。

【0173】

コンテンツ利用装置110cにおける書き出しコンテンツリスト管理部1803は、書き出しコンテンツリスト蓄積部1804のMCLを管理する。具体的には、コンテンツを書き出したとき、書き出したコンテンツのコンテンツIDを書き出しコンテンツリスト受信部1802に渡し、書き出しコンテンツリスト受信部1802が受信したMCLを受け取り、書き出しコンテンツリスト蓄積部1804のMCLを更新する、といった処理を行う。

【0174】

コンテンツ利用装置110cにおける書き出しコンテンツリスト蓄積部1804は、MCLを蓄積する部であり、ハードディスク等によって実現される。 10

以上のように構成されたコンテンツ利用システム4において、MCLをコンテンツ取り込み装置100とコンテンツ利用装置110cとの間で同期する処理を、図22および図23に示すフローチャートを用いて説明する。なお、コンテンツ取り込み装置100におけるコンテンツ取り込み時の処理は、本発明の実施の形態3において、図18で示した動作と同様であるので、ここでは省略する。

【0175】

図22は、コンテンツ利用装置110cにおける、コンテンツの書き出し処理を示すフローチャートである。

分離部111において、コンテンツ取り込み装置100から受け取ったトランスポートストリームから、コンテンツとECMを分離する。また、PMTを分離し、PMTのディスクリフタ部のcontent-id-descriptorからコンテンツIDを取得し、コンテンツ鍵情報復号部112に通知する(ステップS1901)。 20

【0176】

コンテンツ鍵情報復号部112は、分離部111から取得したコンテンツIDを、書き出しコンテンツリスト管理部1803に渡すとともに、書き出しコンテンツリスト管理部1803は、書き出しコンテンツリスト蓄積部1804からMCLを読み出す(ステップS1902)。このとき、書き出しコンテンツリスト蓄積部1804にMCLが蓄積されていなければ、MCLを生成する。

【0177】

書き出しコンテンツリスト管理部1803は、コンテンツ鍵情報復号部112から受け取ったコンテンツIDがMCLに存在するかどうかの検索を行う(ステップS1903)。 30

【0178】

ステップS1903において、NOの場合、すなわちコンテンツIDがMCLに存在しない場合は、当該コンテンツIDを書き出しコンテンツリスト管理部1803において、コンテンツ取り込み装置100に送信するために、一時的に保持する(ステップS1904)。

【0179】

コンテンツ鍵情報復号部112は、分離部111からECMのTSパケットを受け取り、ECMセクションを再構成し、再暗号化されたECMを取得する。ネットワーク鍵とコンテンツIDとのXORをとり、ECMの暗号化部分を復号する(ステップS1905)。 40

【0180】

コンテンツ鍵情報復号部112は、ECMからコンテンツ鍵を取り出し、コンテンツ鍵をコンテンツ復号部116に渡すと共に、コンテンツ出力制御部115に対し、当該コンテンツを書き出し部119へ渡すように指示を行う(ステップS1906)。これにより、コンテンツ出力制御部115は、コンテンツ出力選択部117に対してコンテンツを書き出すように制御する。

【0181】

コンテンツ復号部116は、分離部111から取得したTSパケットを、コンテンツ鍵情報復号部112から取得したコンテンツ鍵で復号(デスクランブル)する(ステップS1 50

907)。

【0182】

コンテンツ出力選択部117は、コンテンツ出力制御部115の制御に基づき、コンテンツを書き出すためのコンテンツ書き出し部119へコンテンツを受け渡す(ステップS1908)。

【0183】

コンテンツ書き出し部119は、コンテンツを蓄積メディアに書き出す(ステップS1909)。具体的には、DVD-RAM、D-VHS等の蓄積メディアに対応した形式で、コンテンツを暗号化したり、フォーマット変換したりして、蓄積メディアにコンテンツを書き出す。

10

【0184】

ステップS1903において、YESの場合、すなわちコンテンツIDがMCLに存在する場合は、MCLの該当コンテンツIDに関する情報を用いて、書き出し可否の確認を行う(ステップS1910)。具体的には、MCLには、コンテンツID毎に書き出し回数、単位時間あたりの書き出し回数の上限などが記録されるようになっているため、これらを参照して、書き出し可能かどうかの確認を行う。

【0185】

ステップS1910において、YESの場合、すなわち書き出し可能と判定された場合は、当該コンテンツIDを書き出しコンテンツリスト管理部1803で一時的に保持する(ステップS1904)。ステップS1904以降の処理の詳細については前述の通りであるので、以降は省略する。

20

【0186】

ステップS1910において、NOの場合、すなわち書き出し不可と判定された場合は、コンテンツ書き出し処理を中止する(ステップS1911)。

ここで、図22におけるステップS1904で示したように、コンテンツ利用装置110cの書き出しコンテンツリスト管理部1803で一時的に保持したコンテンツIDを、コンテンツ取り込み装置100に送信することにより、コンテンツ取り込み装置100とコンテンツ利用装置110cとの間で、MCLの同期をとる処理を示すフローチャートを図23に示す。なお、図23では、複数のコンテンツ利用装置110cの内、コンテンツを書き出したコンテンツ利用装置110cをその代表として示しているが、その他のコンテンツ利用装置110cも新たなMCLを受信し、同期する処理を行う。

30

【0187】

コンテンツ利用装置110cの書き出しコンテンツリスト管理部1803で保持されている、書き出したコンテンツのコンテンツIDは、書き出しコンテンツリスト受信部1802に渡され、ネットワークを通じてコンテンツ取り込み装置100に送信される(ステップS2001)。

【0188】

コンテンツ取り込み装置100の書き出しコンテンツリスト送信部1801は、コンテンツIDを受信し(ステップS2002)、書き出しコンテンツリスト管理部1401に渡す。

40

【0189】

書き出しコンテンツリスト管理部1401は、書き出しコンテンツリスト蓄積部1402のMCLを読み出し(ステップS2003)、受信したコンテンツIDをMCLに追加あるいは更新し、書き出しコンテンツリスト蓄積部1402のMCLを更新する(ステップS2004)。このとき、MCLのバージョンを更新する。更新されたMCLを書き出しコンテンツリスト送信部1801に渡す。

【0190】

書き出しコンテンツリスト送信部1801は、更新されたMCLをコンテンツ利用装置110cに送信する(ステップS2005)。例えば、全てのコンテンツ利用装置110cに対してブロードキャストする方法が挙げられる。

50

【0191】

コンテンツ利用装置110cの書き出しコンテンツリスト受信部1802は、更新されたMCLを受信する(ステップS2006)。受信したMCLを書き出しコンテンツリスト管理部1803に渡す。

【0192】

書き出しコンテンツリスト管理部1803は、受け取ったMCLのバージョンを参照し、保持しているMCLのバージョンとの比較を行う(ステップS2007)。

【0193】

ステップS2007において、YESの場合、すなわち受け取ったMCLのバージョンが新である場合、書き出しコンテンツリスト蓄積部1804のMCLを置換する(ステップS2008)。なお、書き出しコンテンツリスト蓄積部1804にMCLが蓄積されていなかった場合には、無条件で受け取ったMCLを書き込む。

【0194】

ステップS2007において、NOの場合、すなわち受け取ったMCLのバージョンが古い場合、受け取ったMCLを破棄する。

このように、本コンテンツ利用システム4では、ネットワークバインドされたコンテンツにコンテンツIDを付与し、同時にコンテンツ取り込み装置100において管理するMCLにコンテンツIDを登録する。このMCLを各コンテンツ利用装置110cに送信し、コンテンツを書き出す際には、各コンテンツ利用装置110cが保持するMCLを用いて書き出し可否を判定することにより、無制限なコンテンツの書き出しに制限を課するよう

【0195】

(実施の形態5)

以下、本発明の実施の形態5について、図面を用いて詳細に説明する。

図24は、本発明の実施の形態5に係るコンテンツ利用システム5構成を示すブロック図である。なお、本図において、図3に示した実施の形態1のコンテンツ利用システム1と同様の構成要素については、図3において既に説明しているため、図3と同様の符号を付して以下の説明を省略する。

【0196】

本発明における実施の形態1～実施の形態4で挙げたコンテンツ利用システムでは、コンテンツ取り込み装置100で取り込まれたコンテンツは、ネットワークで予め共有された暗号鍵のみを用いてコンテンツ鍵情報を再暗号化しているため、リアルタイムに利用することも可能であるし、ネットワーク上に接続されたハードディスク等の蓄積部に記録した後でコンテンツを利用することも可能であった。そのため、コンテンツを書き出す際にMCLを用いて書き出しに制限を課するようにしていた。

【0197】

それに対し、本発明の実施の形態5で示すコンテンツ利用システム5では、コンテンツ取り込み装置100において、コンテンツ取り込み時に、ある秘密情報を生成し、この秘密情報を作用させてコンテンツ鍵情報を再暗号化し、コンテンツ利用装置110dは、コンテンツを書き出す(再生する)際に、出力先を指定し、コンテンツ取り込み装置100から秘密情報を取得すること、コンテンツを書き出す(再生する)ことができるようにしている。すなわち、コンテンツ利用装置110dからコンテンツ取り込み装置100にコンテンツの出力先を指定し、出力先に従ってコンテンツをリアルタイムに蓄積メディアに書き出す、または再生するモードを設けるようにしたものである。ここで、コンテンツ取り込み装置100において、コンテンツ利用装置110dから出力要求を受けた場合に、書き出し確認を行うことにより、コンテンツの書き出しに制限を課するようになることができる。

【0198】

図24に示すコンテンツ利用システム5は、コンテンツ取り込み装置100が、入力部101と、分離部102と、コンテンツ鍵情報暗号変換部103と、多重化部105と、出

10

20

30

40

50

力要求処理部 2101 とを備え、コンテンツ利用装置 110d が、分離部 111 と、コンテンツ鍵情報復号部 112 と、コンテンツ出力制御部 115 と、コンテンツ復号部 116 と、コンテンツ出力選択部 117 と、コンテンツ出力部としてコンテンツ表示部 118 およびコンテンツ書き出し部 119 と、出力要求部 2102 とを備え、コンテンツ取り込み装置 100 のコンテンツ鍵情報暗号変換部 103 が、任意のタイミングで秘密情報を生成し、ネットワークで予め共有された暗号鍵（ネットワーク鍵）と、前記秘密情報とを用いてコンテンツ鍵情報を暗号化し、コンテンツ利用装置 110d の出力要求部 2102 が、コンテンツの書き出しまたは再生を出力要求としてコンテンツ取り込み装置 100 に出力要求を送信し、コンテンツ取り込み装置 100 の出力要求処理部 2101 が、要求応答として前記秘密情報を送信し、コンテンツ利用装置 110d の出力要求部 2102 が、前記要求応答から前記秘密情報を取得し、コンテンツ鍵情報復号部 112 は、前記ネットワーク鍵と前記秘密情報とを用いてコンテンツ鍵情報を復号し、コンテンツ鍵情報から取得したコンテンツ鍵を用いてコンテンツを復号し、コンテンツ出力選択部 117 は、出力先に応じたコンテンツの出力切り替えを行うことを特徴とする。

10

【0199】

コンテンツ取り込み装置 100 におけるコンテンツ鍵情報暗号変換部 103 は、本発明の実施の形態 1 では、ネットワーク鍵を用いて ECM を暗号変換していたが、本実施の形態では、コンテンツ取り込み時において、任意のタイミングで秘密情報を生成し、ネットワーク鍵と秘密情報を用いて ECM を再暗号化するようにしている。秘密情報を生成するタイミングとして、例えば、番組（イベント）毎、コンテンツ毎に生成し、新たに生成した場合、以前の秘密情報は削除する。このように、秘密情報を有効としたい間だけ秘密情報を保持する方法により、出力するコンテンツを識別することができる。

20

【0200】

コンテンツ取り込み装置 100 における出力要求処理部 2101 は、コンテンツ利用装置 110d からコンテンツの出力要求として、コンテンツの出力先と認証に用いるチャレンジを受信し、チャレンジからレスポンスを生成して、レスポンスと前記秘密情報をコンテンツ利用装置 110d に要求応答として送信する。

【0201】

コンテンツ利用装置 110d における出力要求部 2102 は、コンテンツ取り込み装置 100 に対して、コンテンツを書き出すか、再生するかに応じた出力先と、認証に用いるチャレンジを送信する。出力要求の応答として、コンテンツ取り込み装置 100 からレスポンスと前記秘密情報を受信し、レスポンスを認証する。認証に成功した場合にのみ、前記秘密情報をコンテンツ鍵情報復号部 112 に渡すように処理する。なお、チャレンジ・レスポンス認証については、本実施の形態では詳細に記述していないが、例えば、CHAP（Challenge Handshake Authentication Protocol）や、SSL（Secure Socket Layer）において用いられるチャレンジ・レスポンスと同様の方法で認証処理が行われる。

30

【0202】

以上のように構成されたコンテンツ利用システム 5 の動作を、図 25 および図 26 に示すフローチャートを用いて説明する。

40

図 25 は、コンテンツ取り込み装置 100 における、コンテンツ取り込み時の処理を示すフローチャートである。

【0203】

入力部 101 は、放送波からトランスポートストリームを受信する（ステップ S2201）。

分離部 102 は、入力部 101 からトランスポートストリームを受け取り、TS パケットの PID を参照して、コンテンツの TS パケットと ECM の TS パケットを分離する（ステップ S2202）。また、コンテンツ鍵情報暗号変換部 103 がイベントを識別することを可能とするため、EIT のパケットを分離してコンテンツ鍵情報暗号変換部 103 に渡す。

50

【0204】

コンテンツ鍵情報暗号変換部103は、ECMのTSパケットを受け取り、ECMセクションを再構成し、ワーク鍵を用いて暗号化されたECMを復号する（ステップS2203）。また、受け取ったEITのTSパケットからEITを再構成し、イベント情報を取得する。

【0205】

コンテンツ鍵情報暗号変換部103は、イベント単位で秘密情報を生成する（ステップS2204）。具体的には、コンテンツ鍵情報暗号変換部103は、イベント毎に乱数で一定バイト長の秘密情報を生成する。

【0206】

コンテンツ鍵情報暗号変換部103は、生成した秘密情報とネットワーク鍵とを用いて、ECMを再暗号化する（ステップS2205）。具体的には、生成した秘密情報とある暗号アルゴリズム（例えばAES等）を用いて、ECMのコンテンツ鍵の部分で暗号化する。さらに、ECM全体をネットワーク鍵で暗号化する。この再暗号化されたECMをTSパケット化し、多重化部105に渡す。

【0207】

多重化部105は、分離部102から受け取ったコンテンツのTSパケットと、コンテンツ鍵情報暗号変換部103から受け取った暗号変換後のECMのTSパケットとを多重化する（ステップS2206）。

【0208】

このように、コンテンツ取り込み装置100では、秘密情報を生成し、ECMをネットワーク鍵と秘密情報とを用いて暗号変換することにより、秘密情報を取得しない限りコンテンツの利用ができないように処理される。

【0209】

一方、図26は、コンテンツ利用装置110dにおける、コンテンツ書き出し時の処理を示すフローチャートである。

コンテンツ利用装置110dの出力要求部2102は、リアルタイムの放送コンテンツを直接書き出す場合、コンテンツ取り込み装置100と認証処理を行うためのチャレンジ（例えば乱数）を生成し、チャレンジデータとコンテンツの出力先（コンテンツ書き出し部119を指定する等）とを出力要求として、コンテンツ取り込み装置100に送信する（ステップS2301）。

【0210】

コンテンツ取り込み装置100の出力要求処理部2101は、コンテンツ利用装置110dからの出力要求として、チャレンジと出力先を受信する（ステップS2302）。

【0211】

出力要求処理部2101は、コンテンツの出力可否を判定する（ステップS2303）。具体的には、出力要求に含まれる出力先（書き出し先）を確認し、放送波に記述されるコピー制御情報やシステムで規定された書き出し先の制約と比較することにより、書き出し可能かどうかを決定する。また、あるコンテンツ利用装置110dとのチャレンジ・レスポンスを行った場合、ネットワーク上の他のコンテンツ利用装置110dからのチャレンジを受け付けない、あるいは、一定数のコンテンツ利用装置110dからのチャレンジまでは受け付けるようにすることにより、コンテンツの書き出しに制限を課するようにできる。

【0212】

ステップS2303において、YESの場合、すなわち出力可と判定された場合には、チャレンジからレスポンスを生成し、要求応答として、レスポンスと秘密情報をメッセージに設定する（ステップS2304）。

【0213】

ステップS2303において、NOの場合、すなわち出力不可と判定された場合には、その旨を示すエラーメッセージを生成し、要求応答としてメッセージに設定する。

10

20

30

40

50

【0214】

出力要求処理部2101は、要求応答をコンテンツ利用装置110dに送信する（ステップS2305）。

コンテンツ利用装置110dの出力要求部2102は、要求応答を受信し（ステップS2306）、レスポンスを認証する（ステップS2307）。

【0215】

ステップS2307において、YESの場合、すなわち認証処理が成功した場合は、秘密情報を取得し、コンテンツ鍵情報復号部112に渡す（ステップS2308）。

【0216】

ステップS2307において、NOの場合、すなわち認証処理が失敗した場合は、秘密情報を取得せず、コンテンツの書き出し処理を終了する。

コンテンツ鍵情報復号部112は、ネットワーク鍵を用いて再暗号化されたECMを復号し、さらに秘密情報を用いて、さらに暗号化されているコンテンツ鍵の部分を復号する（ステップS2309）。また、コンテンツ出力制御部115に対し、コンテンツの書き出し先、書き出し経路などを指示する。

【0217】

コンテンツ鍵情報復号部112は、復号されたコンテンツ鍵をコンテンツ復号部116に渡す（ステップS2310）。

コンテンツ復号部116は、分離部111から受け取った暗号化コンテンツを、コンテンツ鍵情報復号部112から受け取ったコンテンツ鍵で復号する（ステップS2311）。

【0218】

コンテンツ出力選択部117は、コンテンツ出力制御部115からのコンテンツ出力制御情報（コンテンツの書き出し先、書き出し経路など）に従い、コンテンツ書き出し部119にコンテンツを出力するよう選択する（ステップS2312）。

【0219】

コンテンツ書き出し部119は、コンテンツを蓄積メディアに出力する（ステップS2313）。

このように、本コンテンツ利用システム5では、リアルタイムに蓄積メディアに出力する（もしくは再生する）モードを設け、コンテンツ取り込み時に生成した秘密情報と、ネットワーク鍵とを用いてコンテンツ鍵情報を再暗号化することにより、秘密情報を取得できたコンテンツ利用装置110dでしかコンテンツを利用できないようにしている。すなわち、コンテンツ取り込み装置100が、限られたコンテンツ利用装置110dにしか秘密情報を渡さないように制御すれば、MCLの蓄積や管理が不要であるため、構成をシンプルにすることができ、また、安全性が高いといった利点がある。例えば、複製が1回しか許されていないコンテンツ（コピー制御情報がNETWORK COPYである等）の場合、コンテンツを取り込む際にコピー制御情報を参照することによって本モードを適用してコンテンツ鍵情報を暗号変換し、コンテンツ取り込み装置100が唯一つのコンテンツ利用装置110dのみに秘密情報を渡すようにすると、ネットワークからは複製が1つのみ作れる、といったような制約を課することができる。

【0220】

なお、本実施の形態では、コンテンツ取り込み装置100においてコンテンツ鍵情報を暗号化する際、コンテンツ取り込み時に生成した秘密情報と、ネットワーク上で予め共有された暗号鍵であるネットワーク鍵とを用いて暗号化を行なう場合の例を示したが、少なくともコンテンツ取り込み装置100とコンテンツ利用装置110dとが共有する暗号鍵であれば、特にこれに限定されるものではない。

【0221】

（実施の形態6）

以下、本発明の実施の形態6について、図面を用いて詳細に説明する。

図27は、本発明の実施の形態6に係るコンテンツ利用システム6構成を示すブロック図である。なお、本図において、図3に示した実施の形態1のコンテンツ利用システム1と

10

20

30

40

50

同様の構成要素については、図 3 において既に説明しているのので、図 3 と同様の符号を付して以下の説明を省略する。

【0222】

図 27 に示すコンテンツ利用システム 6 は、本発明の実施の形態 1 に挙げたコンテンツ利用システム 1 に対して、さらに、コンテンツを蓄積メディアに書き出す記録装置 2401 とで構成され、コンテンツ取り込み装置 100 の構成は、本発明の実施の形態 1 でのコンテンツ取り込み装置 100 と同様であるが、コンテンツ利用装置 110e は、書き出しコンテンツリスト管理部 113 と、書き出しコンテンツリスト蓄積部 114 と、コンテンツ書き出し部 119 とが省かれており、記録装置 2401 が、コンテンツ書き出し部 2402 と、書き出しコンテンツリスト管理部 2403 と、書き出しコンテンツリスト蓄積部 2404 とを備え、記録装置 2401 が MCL を管理し、コンテンツ利用装置 110e から受信したコンテンツとコンテンツ ID を蓄積メディアに書き出すとき、MCL を用いてコンテンツの書き出し可否を判定し、書き出し可否判定の結果に基づいて、コンテンツの書き出しを制御することとを特徴とする。

【0223】

記録装置 2401 は、例えば、DVD-RAM レコーダや、SD カードリーダー/ライターなど、蓄積メディアへコンテンツを書き込むための装置が挙げられる。コンテンツ書き出し部 2402 は、コンテンツを蓄積メディアに書き出すために必要な処理を行い、蓄積メディアにコンテンツを書き出す。

【0224】

書き出しコンテンツリスト蓄積部 2404 は、MCL を蓄積しておく部であり、ハードディスク等によって実現される。

書き出しコンテンツリスト管理部 2403 は、書き出しコンテンツリスト蓄積部 2404 に蓄積される MCL を管理する。具体的には、書き出しコンテンツリスト蓄積部 2404 から MCL を読み出し、MCL を更新して書き出しコンテンツリスト蓄積部 2404 に書き込む、といった MCL の読み書き処理や、蓄積メディアに書き出すコンテンツのコンテンツ ID をコンテンツ書き出し部 2402 から受け取り、MCL を用いてコンテンツが蓄積メディアに書き出せるかどうかの判定を行う。

【0225】

以上のように構成されたコンテンツ利用システム 6 の動作を、図 28 に示すフローチャートを用いて説明する。

なお、コンテンツ取り込み装置 100 におけるコンテンツ取り込み処理については、本発明の実施の形態 1 と同様であり、既に説明しているため、ここでは説明を省略する。

【0226】

図 28 は、コンテンツ利用装置 110e および記録装置 2401 における、コンテンツ書き出し処理を示すフローチャートである。

分離部 111 において、コンテンツ取り込み装置 100 から受け取ったトランスポートストリームから、コンテンツと ECM を分離する（ステップ S2501）。

【0227】

コンテンツ鍵情報復号部 112 は、分離部 111 から ECM の TS パケットを受け取り、ECM セクションを再構成し、再暗号化された ECM を取得する。ECM の暗号化部分を予め取得してあるネットワーク鍵で復号する（ステップ S2502）。

【0228】

コンテンツ鍵情報復号部 112 は、ECM からコンテンツ鍵を取り出し、コンテンツ鍵をコンテンツ復号部 116 に渡す（ステップ S2503）。また、コンテンツ出力制御部 115 に対し、コンテンツ出力選択部 117 でコンテンツを記録装置 2401 に出力するよう制御するため、書き込み先、書き込み経路などの情報を送信する。さらに、記録装置 2401 で、コンテンツ書き込み可否の判定に用いるコンテンツ ID を ECM から読み出し、コンテンツ出力制御部 115 に渡す。コンテンツ出力制御部 115 は、コンテンツ ID と、書き込み先と、書き込み経路とをコンテンツ出力制御情報として、コンテンツ出力選

10

20

30

40

50

沢部 1 1 7 に送信する。

【0229】

コンテンツ復号部 1 1 6 は、分離部 1 1 1 から取得した TS パケットを、コンテンツ鍵情報復号部 1 1 2 から取得したコンテンツ鍵で復号（デスクランブル）する（ステップ S 2 5 0 4）。

【0230】

コンテンツ出力選択部 1 1 7 は、コンテンツ出力制御部 1 1 5 からのコンテンツ出力制御情報に基づき、記録装置 2 4 0 1 へ出力を切り替え（ステップ S 2 5 0 5）、コンテンツとコンテンツ出力制御情報を送信する（ステップ S 2 5 0 6）。

【0231】

記録装置 2 4 0 1 のコンテンツ書き出し部 2 4 0 2 は、コンテンツ利用装置 1 1 0 e から、コンテンツとコンテンツ出力制御情報を受信する（ステップ S 2 5 0 7）。受信したコンテンツ出力制御情報を、書き出しコンテンツリスト管理部 2 4 0 3 に渡す。

【0232】

書き出しコンテンツリスト管理部 2 4 0 3 は、書き出しコンテンツリスト蓄積部 2 4 0 4 から MCL を読み出し（ステップ S 2 5 0 8）、書き出し可否判定を行う（ステップ S 2 5 0 9）。この書き出し可否判定は、本発明における実施の形態 1 で説明した方法と同様であるので、ここでは省略する。

【0233】

ステップ S 2 5 0 9 において、YES の場合、すなわち書き出し可能と判定された場合は、MCL を更新し、書き出しコンテンツリスト蓄積部 2 4 0 4 に蓄積する（ステップ S 2 5 1 0）。また、コンテンツ書き込み処理の開始をコンテンツ書き出し部 2 4 0 2 に指示する。

【0234】

コンテンツ書き出し部 2 4 0 2 は、コンテンツを蓄積メディアに書き出す（ステップ S 2 5 1 1）。

なお、ステップ S 2 5 0 9 において、NO の場合、すなわち書き出し不可と判定された場合は、コンテンツ書き出し処理を終了する。

【0235】

このように、本コンテンツ利用システム 6 では、記録装置 2 4 0 1 で MCL を管理し、コンテンツを書き出す際に MCL を用いて書き出し可否判定を行うことにより、レコーダ毎にコンテンツ書き出しの制限を課するようになっている。

【0236】

なお、コンテンツ ID の生成方法について、コンテンツ ID が単調増加または単調減少となるような生成部であれば、本発明における実施の形態 1 ～実施の形態 4、および、実施の形態 6 で示した方法に限定されるものではない。また、コンテンツ ID がユニークな乱数値となるように生成しても良い。

【0237】

また、コンテンツ ID の付与単位について、コンテンツのスクランブル単位でコンテンツ ID を付与しても良い。あるいは、ユーザによる再生、録画等のボタン操作（ユーザのアクション）が行われる単位、具体的には、ユーザが録画開始を指示してから録画終了を指示するまで、あるいは、ユーザがあるチャネルを選択してから他のチャネルを選択するまで、などの単位でコンテンツ ID を付与するようにしても良い。

【0238】

また、本発明における実施の形態 1 ～実施の形態 4、および、実施の形態 6 では、コンテンツ取り込み装置 1 0 0 のコンテンツ ID 生成部 1 0 4 においてコンテンツ ID を生成する場合の例を示したが、コンテンツ ID 生成部 1 0 4 を備えず、入力データ（例えば、EIT 等のコンテンツと共に配信されるデータ）に予め付与されている情報をコンテンツ ID として用いても良い。具体的には、デジタル放送の場合では、EIT に設定されている service_id と event_id とをそのままコンテンツ ID として利用したり

10

20

30

40

50

、送信側でコンテンツに付与したコンテンツIDが配信される場合は、このコンテンツIDを利用して良い。

【0239】

また、本実施の形態では、コンテンツとコンテンツ鍵情報の対応付けを、多重化部105を用いて行う例を示したが、この手法はこの例に限られたものではなく、分離・多重を行わず、何らかの方法でコンテンツとコンテンツ鍵情報の対応付けをとっても良い。

【0240】

また、コンテンツ取り込み装置100とコンテンツ利用装置110との間、あるいは、複数のコンテンツ利用装置110間、あるいは、コンテンツ利用装置110と記録装置2401との間で、MCLの確認を行うためにコンテンツIDを送受信したり、MCLの同期情報を送受信したり、コンテンツを送受信したり、コンテンツ出力制御情報を送受信したりするが、データの差し替え、改ざん防止のため、これらの通信の暗号化を行っても良い。

【0241】

また、少なくともコンテンツ取り込み装置100におけるコンテンツ鍵情報暗号変換部103、コンテンツID生成部104や、コンテンツ利用装置110におけるコンテンツ鍵情報復号部112、書き出しコンテンツリスト管理部118、書き出しコンテンツリスト蓄積部114、コンテンツ出力制御部115は、セキュリティに係る処理を行う部であるため、セキュリティモジュールなどの耐タンパ化されたモジュールで実現しても良い。

【0242】

また、本発明における実施の形態1～実施の形態4では、コンテンツ利用装置110がコンテンツ表示部118とコンテンツ書き出し部119を備える場合の例を示したが、必ずしも両方を備える必要はなく、コンテンツ表示部118のみを備えるコンテンツ利用装置110や、コンテンツ書き出し部119のみを備えるコンテンツ利用装置110などであっても良い。この場合、コンテンツ出力制御部115あるいはコンテンツ出力選択部117の一方、または、両方を省略することもできる。

【0243】

さらに、本発明における実施の形態1～実施の形態6では、デジタル放送からMPEG-2 8×Sで多重化されたMPEGコンテンツを取り込む場合の例を示したが、本発明はこれに限られたものではなく、インターネット等の通信媒体やパッケージメディア等の記録媒体から任意のフォーマットのコンテンツを取り込む場合にも適用可能であることは言うまでもない。

【0244】

また、上記各実施の形態において、コンテンツ出力として、コンテンツをモニターに再生表示する表示部と、蓄積メディアに書き出す書き出し部とを有する例を示したが、これに限らず、IEEE1394等のデジタルバスに出力するようにしてもよい。このデジタルバスに出力する場合も、各実施形態における書き出し部と同様に出力可否を判定する構成とすればよい。

【0245】

さらに、上記各実施の形態におけるコンテンツ利用装置において、コンテンツ書き出し部は、ネットワークがコンテンツにバインドされていない状態での書き出しに加えて、バインドされた状態での書き出しをユーザの選択に応じて行う構成としてもよい。

【0246】

また、上記各実施の形態におけるMCLのサイズが最大サイズに達し、コンテンツIDを追加できなくなった場合に、MCLから削除すべきコンテンツIDを乱数により決定して削除する構成としてもよい。

【0247】

さらに、上記各実施形態では、ECM中に書き出し条件として最大書き出し回数、書き出し先、書き出し経路を設定可能であるが、書き出しの可否を示す情報をトランスポートストリーム中のECM以外に設定する構成としてもよい。

【0248】

また、上記各実施の形態におけるコンテンツ取り込み装置は、何れかのコンテンツ利用装置と物理的に一体であってもよい。

【0249】

(産業上の利用可能性)

本発明におけるコンテンツ利用システムは、ネットワークに接続されたコンテンツ取り込み装置と1以上のコンテンツ利用装置とからなる。コンテンツ取り込み装置は、コンテンツIDを発行するコンテンツID発行部と、ネットワーク上で予め共有されたネットワーク鍵でコンテンツ鍵情報を暗号変換するコンテンツ鍵情報暗号変換部とを備える。コンテンツ利用装置は、暗号変換されたコンテンツ鍵情報をネットワーク鍵で復号するコンテンツ鍵情報復号部と、蓄積メディアに書き出したコンテンツのコンテンツIDを記した書き出しコンテンツリスト(MCL)を蓄積する書き出しコンテンツリスト蓄積部と、MCLに基づきコンテンツの書き出し可否判定を行う書き出しコンテンツリスト管理部とを備える。本発明は、上記の書き出し可否判定に従ってコンテンツの書き出しを行うコンテンツ利用システム、コンテンツ利用方法、コンテンツ利用装置、コンテンツ利用プログラムとして利用される。

【0250】

【発明の効果】

本発明のコンテンツ利用システムによれば、ネットワークにバインドされたコンテンツ毎に、コンテンツIDを付与して、コンテンツの書き出しテーブルによって管理するので、書き出し手段によって無制限に書き出しすることを抑制することができる。つまり、ネットワークにバインドされていない状態で書き出すことを制限することができる。例えば、家庭内のネットワークにバインドされたコンテンツを蓄積メディアに書き出したいという個人ユーザの要求を満たしながらも著作権を十分に保護することができるので、ユーザの私的利用と著作権者との間の相対立する利益をバランスよく満たすことができる。

【0251】

また、抑制手段は前記テーブルに当該コンテンツIDが既に存在していれば、前記書き出し手段に対して当該コンテンツの書き出しを抑制するので、書き出し手段による書き出しをコンテンツ毎に1回許可し、2回目以降を禁止することができる。

【0252】

また、抑制手段は、前記テーブルに当該コンテンツIDが存在し、かつ書き出し回数が予め定められた最大回数に達していれば、書き出し手段による書き出しを抑制するので、書き出し手段による書き出しをコンテンツ毎に最大回数の範囲内で許可し、それを超える場合は禁止することができる。最大回数は1つの値を予め決めておいてもよいし、コンテンツ毎に予め決めておいてもよいので、ユーザと著作権者との相対立する利益をより柔軟にバランスをとることができる。

【図面の簡単な説明】

【図1】本実施の形態に係るコンテンツ利用システムの全体の構成を示す図である。

【図2】本実施の形態に係るコンテンツ利用システムの全体の構成を示す図である。

【図3】実施の形態1に係るコンテンツ取り込み装置およびコンテンツ利用装置の構成を示す機能ブロック図である。

【図4】実施の形態1に係るECMセクションおよびECMの構成を示す図である。

【図5】実施の形態1に係る書き出しコンテンツリストの構成を示す図である。

【図6】実施の形態1に係るコンテンツ取り込み装置におけるコンテンツ取り込み処理を示すフローチャートである。

【図7】実施の形態1に係るコンテンツ利用装置におけるコンテンツ書き出し処理を示すフローチャートである。

【図8】実施の形態1に係るコンテンツ利用装置におけるコンテンツ再生処理を示すフローチャートである。

【図9】実施の形態1に係るコンテンツ利用装置におけるコンテンツ書き出し処理でのス

10

20

30

40

50

クランブルID生成、記録処理を示すフローチャートである。

【図10】実施の形態1に係るコンテンツ利用装置における書き出し再開処理を示すフローチャートである。

【図11】実施の形態2に係るコンテンツ取り込み装置およびコンテンツ利用装置の構成を示す機能ブロック図である。

【図12】実施の形態2に係るコンテンツ利用装置間での書き出しコンテンツリスト同期処理を示すフローチャートである。

【図13】実施の形態2に係る第1のコンテンツ利用装置での書き出しコンテンツリストの構成を示す図である。

【図14】実施の形態2に係る第2のコンテンツ利用装置の書き出しコンテンツリストの構成を示す図である。 10

【図15】実施の形態2に係る書き出し同期情報示す図である。

【図16】実施の形態3に係るコンテンツ取り込み装置およびコンテンツ利用装置の構成を示す機能ブロック図である。

【図17】実施の形態3に係るPMTおよびコンテンツIDを記述したcontent-id-descriptorの構成を示す図である。

【図18】実施の形態3に係るコンテンツ取り込み装置におけるコンテンツ取り込み処理を示すフローチャートである。

【図19】実施の形態3に係る書き出しコンテンツリストの構成を示す図である。

【図20】実施の形態3に係るコンテンツ利用装置におけるコンテンツ書き出し処理を示すフローチャートである。 20

【図21】実施の形態4に係るコンテンツ取り込み装置およびコンテンツ利用装置の構成を示す機能ブロック図である。

【図22】実施の形態4に係るコンテンツ利用装置におけるコンテンツ書き出し処理を示すフローチャートである。

【図23】実施の形態4に係るコンテンツ取り込み装置およびコンテンツ利用装置間での書き出しコンテンツリスト同期処理を示すフローチャートである。

【図24】実施の形態5に係るコンテンツ取り込み装置およびコンテンツ利用装置の構成を示す機能ブロック図である。

【図25】実施の形態5に係るコンテンツ取り込み装置におけるコンテンツ取り込み処理を示すフローチャートである。 30

【図26】実施の形態5に係るコンテンツ利用装置におけるコンテンツ書き出し処理を示すフローチャートである。

【図27】実施の形態6に係るコンテンツ取り込み装置およびコンテンツ利用装置および記録装置の構成を示す機能ブロック図である。

【図28】実施の形態6に係るコンテンツ利用装置および記録装置におけるコンテンツ書き出し処理を示すフローチャートである。

【符号の説明】

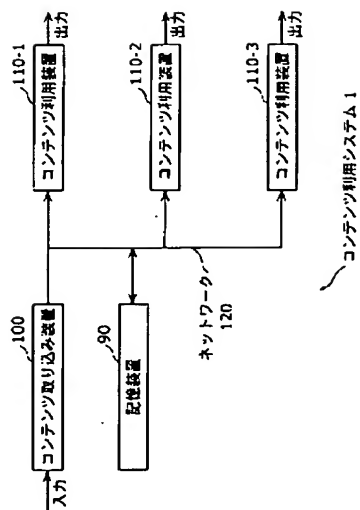
- 1 コンテンツ利用システム
- 90 記憶装置
- 100 コンテンツ取り込み装置
- 101 入力部
- 102 分離部
- 103 コンテンツ鍵情報暗号変換部
- 104 コンテンツID生成部
- 105 多重化部
- 110 コンテンツ利用装置
- 111 分離部
- 112 コンテンツ鍵情報復号部
- 113 書き出しコンテンツリスト管理部

40

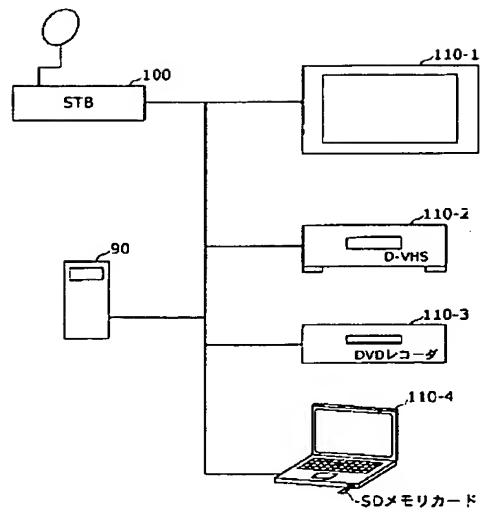
50

1 1 4	書き出しコンテンツリスト蓄積部
1 1 5	コンテンツ出力制御部
1 1 6	コンテンツ復号部
1 1 7	コンテンツ出力選択部
1 1 8	コンテンツ表示部
1 1 9	コンテンツ書き出し部
1 2 0	ネットワーク

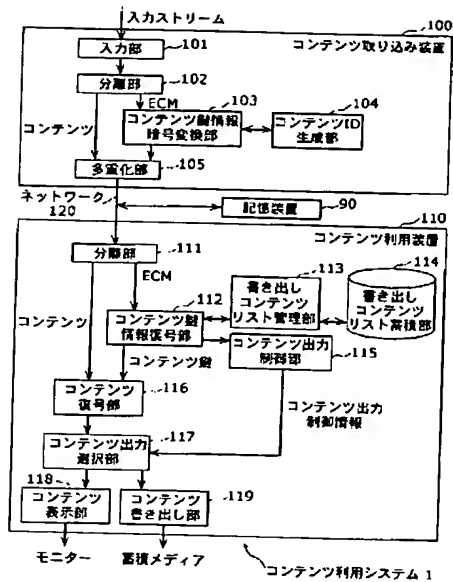
【図 1】



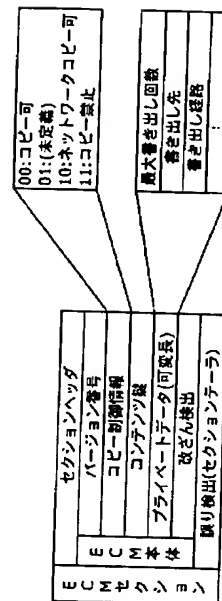
【図 2】



【図 3】



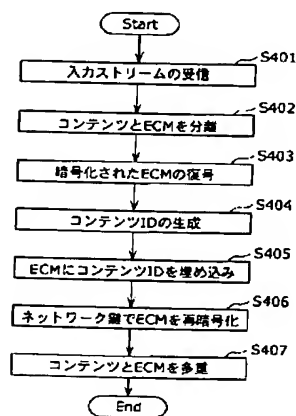
【図 4】



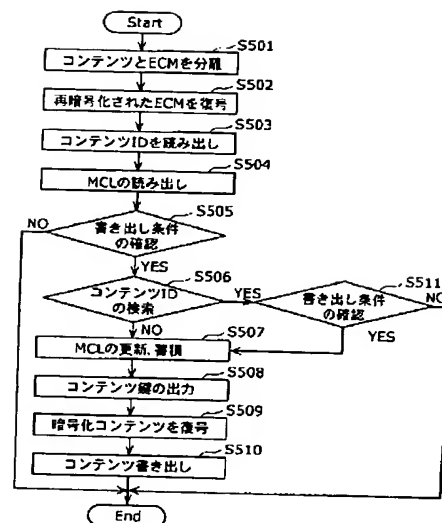
【図 5】

コンテンツID	書き出し回数	書き出し先	書き出し経路
CONTENT-ID-11111	1	-	-
CONTENT-ID-22222	2	DVD-RAM	-
CONTENT-ID-88888	1	-	Digital(SD)
CONTENT-ID-55555	1	-	Analog
CONTENT-ID-77777	3	SDカード	-

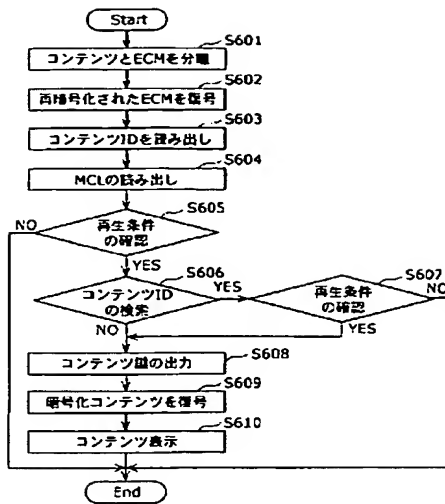
【図 6】



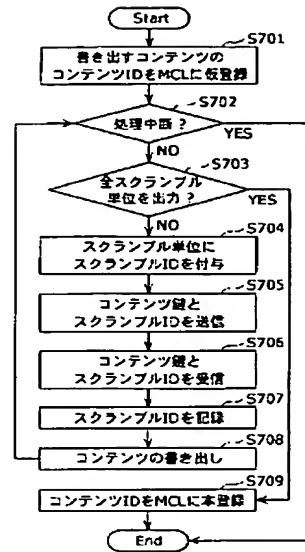
【図 7】



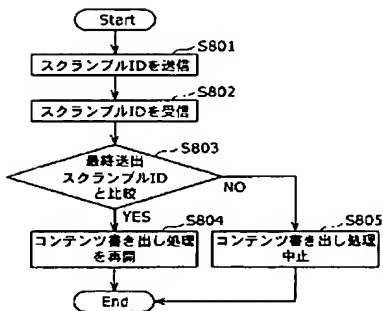
【図 8】



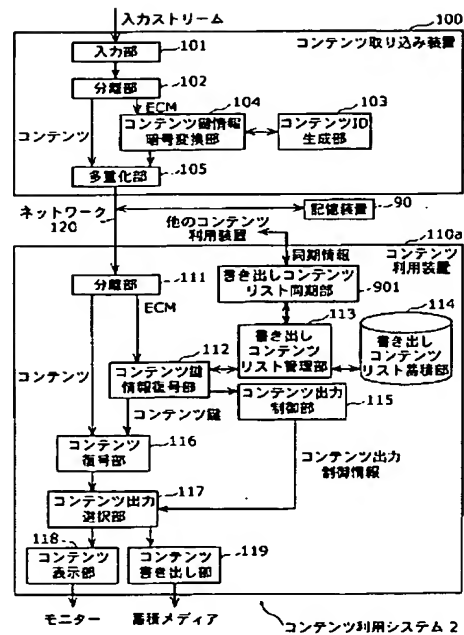
【図 9】



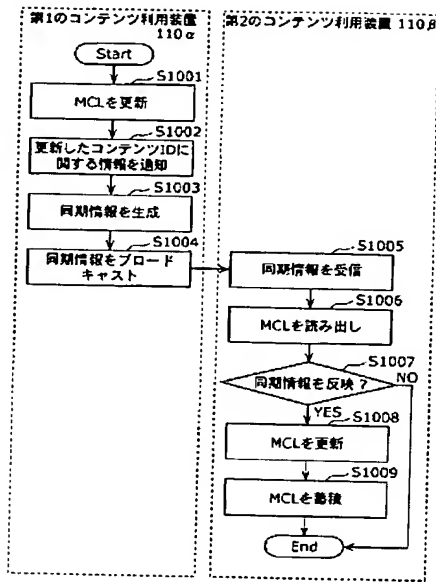
【図 10】



【図 11】



【図12】



【図13】

コンテンツID	書き出し回数/最大書き出し回数	書き出し先	書き出し経路
CONTENT-ID-11111	1/3	-	-
CONTENT-ID-22222	2/2	DVD-RAM	-
CONTENT-ID-88888	1/3	-	Digital(SD)
CONTENT-ID-55555	1/1	-	Analog
CONTENT-ID-12345	1/3	-	-

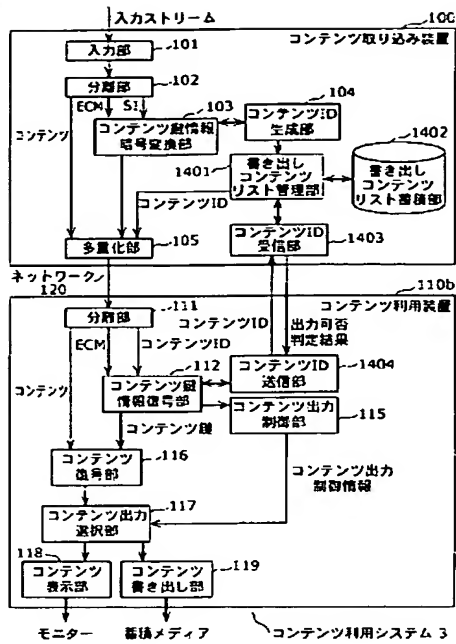
【図14】

コンテンツID	書き出し回数/最大書き出し回数	書き出し先	書き出し経路
CONTENT-ID-11111	1/3	-	-
CONTENT-ID-22222	2/2	DVD-RAM	-
CONTENT-ID-88888	1/3	-	Digital(SD)
CONTENT-ID-55555	1/1	-	Analog

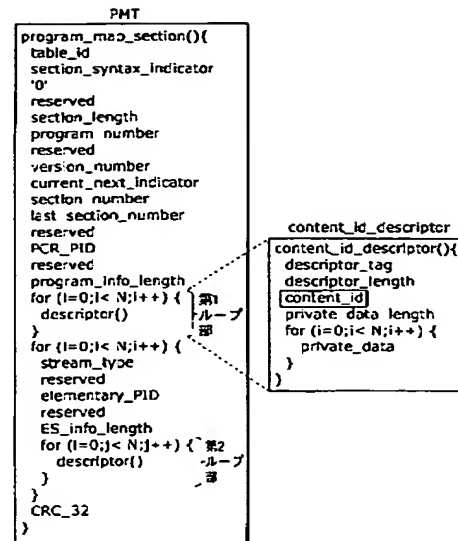
【図15】

同期情報 1301	
SESSION-ID-00240	セッションID
TERMINAL-ID-00001	同期情報送信元のコンテンツ利用装置ID
CONTENT-ID-12345	コンテンツID
1	書き出し回数
-	書き出し先
-	書き出し経路

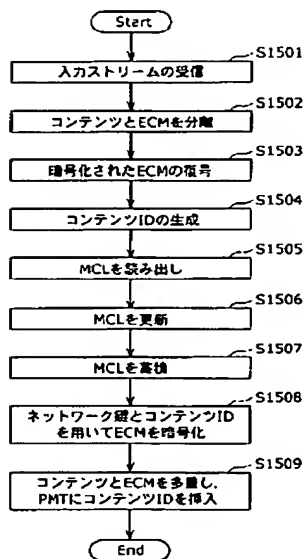
【図16】



【図17】



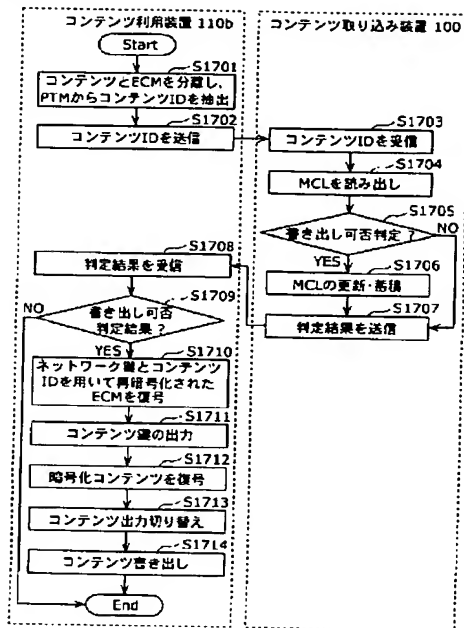
【図18】



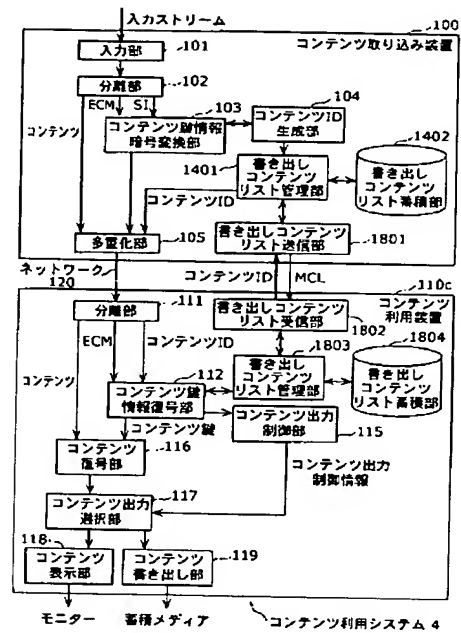
【図19】

コンテンツID	書き出し回数	上取回数/単位	ペナルティ時間	初回書き出し時刻
CONTENT-ID-11111	1	2/Day	1hour	22:22:22
CONTENT-ID-22222	2	3/Day	30min	12:05:12
CONTENT-ID-88888	0	3/Day	1hour	11:11:11
CONTENT-ID-55555	1	3/Day	1hour	1:02:03
CONTENT-ID-77777	0	1/Day	-	-

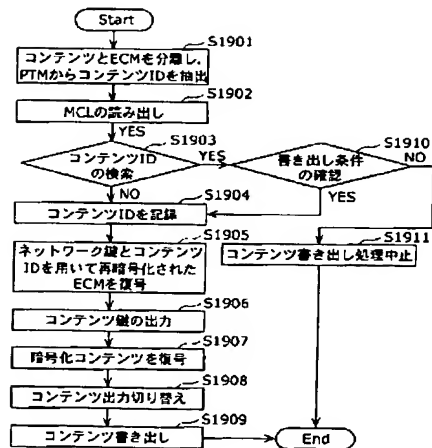
【図 20】



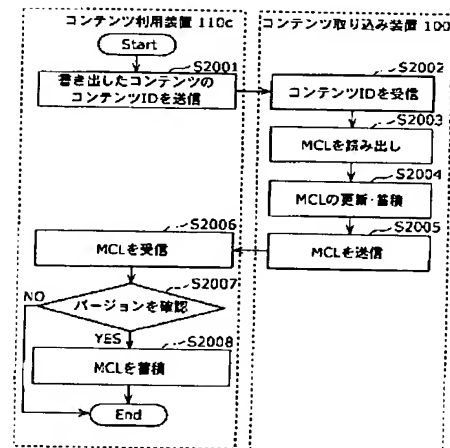
【図 21】



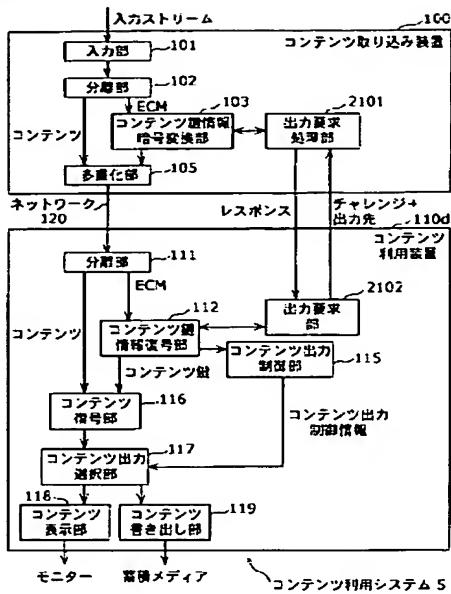
【図 22】



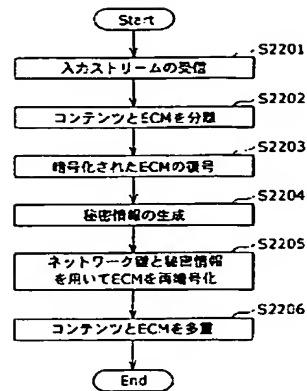
【図 23】



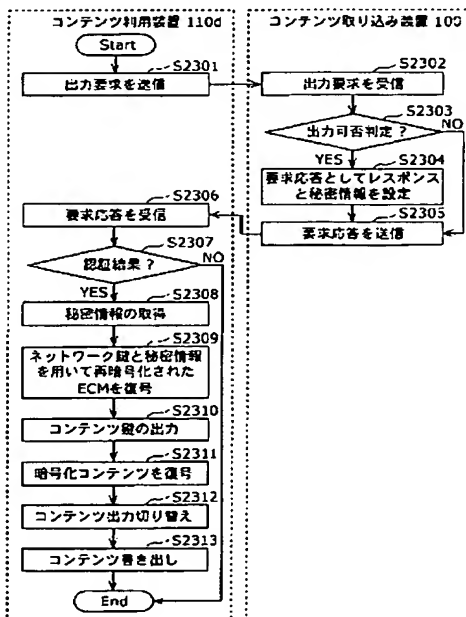
【 2 4 】



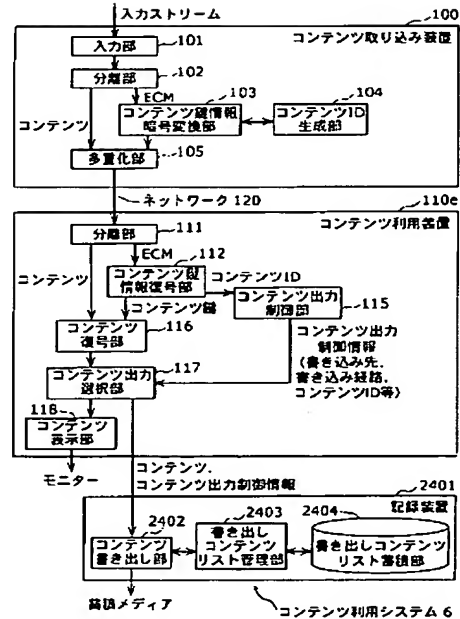
【 2 5 】



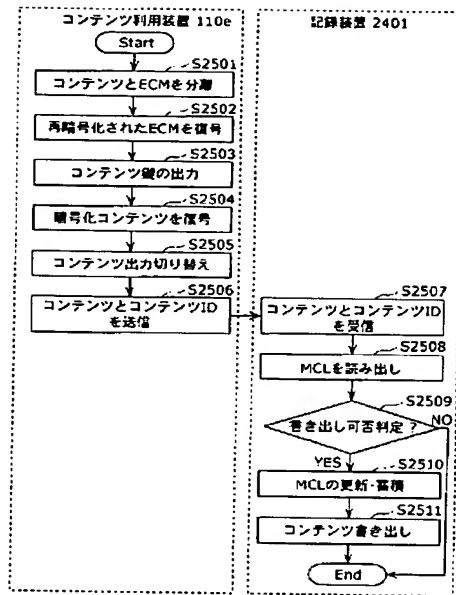
【 ㊦ 2 6 】



【 ㊦ 2 7 】



【図 28】



フロントページの続き

(51)Int.Cl.⁷

F I

テーマコード (参考)

H 0 4 L 9/00 6 0 1 E

(72)発明者 井上 光啓

大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

Fターム(参考) 5B017 AA06 BA05 BB10 CA16

5J104 AA12 AA15 PA07 PA14

BEST AVAILABLE COPY

THIS PAGE BLANK (USPTO)